A BLACK HOLE ATTACK MODEL FOR REACTIVE AD-HOC PROTOCOLS

THESIS

Christopher W. Badenhop

AFIT/GCO/ENG/12-01

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

The views expressed in this Thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government. This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

AFIT/GCO/ENG/12-01

A BLACK HOLE ATTACK MODEL FOR REACTIVE AD-HOC PROTOCOLS

THESIS

Presented to the Faculty

Department of Electrical & Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science

Christopher W. Badenhop

BS in Computer Science and Engineering

MS in Computer Engineering

March 2012

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT/GCO/ENG/12-01

A BLACK HOLE ATTACK MODEL FOR REACTIVE AD-HOC PROTOCOLS

Christopher W. Badenhop

Approved:

Dr. Barry E. Mullins, (Chairman) Date

Major Todd R. Andel, Ph.D USAF (Member) Date

Dr. Timothy H. Lacey, (Member) Date

AFIT/GCO/ENG/12-01

Abstract

Net-Centric Warfare places the network in the center of all operations, making it a critical resource to attack and defend during wartime. This thesis examines one particular network attack, the Black Hole attack, to determine if an analytical model can be used to predict the impact of this attack on ad-hoc networks. An analytical Black Hole attack model is developed for reactive ad-hoc network protocols DSR and AODV. To simplify topology analysis, a hypercube topology is used to approximate ad-hoc topologies that have the same average node degree. An experiment is conducted to compare the predicted results of the analytical model against simulated Black Hole attacks on a variety of ad-hoc networks. The results show that the model describes the general order of growth in Black Hole attacks as a function of the number of Black Holes in a given network. The model accuracy maximizes when both the hypercube approximation matches the average degree and number of nodes of the ad-hoc topology. For this case, the model falls within the 95% confidence intervals of the estimated network performance loss for 17 out of 20 measured scenarios for AODV and 7 out of 20 for DSR.

Acknowledgments

To all who have assisted in the completion of this Thesis: my thanks. This includes the guidance, inspirational seeds, and enduring patience my faculty advisor, Dr. Barry Mullins, and thesis committee have shown me. I am also forever grateful to be employed in the Air Force Research Laboratory, which both encourages and provides individual technical growth and achievement as a core value of its mission in support of the Air Force. Moreover, my direct supervisors and colleagues at AFRL have provided an indispensible pool of morale and technical support which has enabled me to complete work that I believe makes a significant contribution to the Air Force.

Christopher W. Badenhop

Table of Contents

Page

Abstract iv

Acknowledgments v

Table of Contents vi

List of Figures viii

List of Tables ix

I. Introduction 1

1.1 Hypothesis and Goals 3

1.2 Contributions 4

1.3 Structure of the Thesis 5

II. Literature Review 6

2.1 Ad-Hoc Networks and Routing 6

2.2 Black Hole Packet-Drop Attack 14

2.3 Modeling and Simulation of Black Holes in Ad-hoc Networks 18

III. Analytical Model for Black Hole Attacks 30

3.1 Analytical Model Assumptions 31

3.2 Optimization of Black Hole Attacks for Reactive Protocols 32

3.3 Black Hole Attack Predicate for Route Selection by Hop Count Metric 40

3.4 The Hypercube Topology Approximation for Ad-Hoc Topologies 44

3.5 Analytical Black Hole Model for Attractor Phase 53

3.6 A Simple Model for the Exploitation Phase in Hypercube Networks 59

IV. Methodology 63

4.1 System Under Test 63

4.2 Design of Experiment 69

V. Results and Analysis 79

5.1 Experiment Results and Observations 79

5.2 Consideration of Number of Nodes as Alternative Network Parameter 87

5.3 Summary of Findings 93

5.4 Conclusions on the Hypothesis 94

VI. Conclusion 95

6.1 Summary of Work Performed 95

6.2 Accomplishments 96

6.3 Recommendations for Future Work 97

Bibliography 99

List of Figures

Figure Page

1. Ad-hoc Routing Protocol Architecture.. 7

2. Black Hole Attack on Ad-hoc Routing Protocols.. 14

3. Two-hop neighbors in a 2-cube, 3-cube, and 4-cube topology........................... 48

4. Comparison of Hop-Distance Density Functions... 52

5. Attractor Model Results.. 58

6. System Under Test Validation using Cai's Experiment................................... 69

7. Packet Loss Percentage for 10 groups with 50 replications............................ 75

8. Areas for 40 Node Network to Achieve Node Degree......................................77

9. 4-Cube Model versus Ad-hoc Network with Average Degree 4........................ 80

10. 6-Cube Model versus Ad-hoc Network with Average Degree 6..................... 81

11. 8-Cube Model versus Ad-hoc Network with Average Degree 8........................ 82

12. 10-Cube Model versus Ad-hoc Network with Average Degree 10..................... 83

13. Residual Error of the Analytical Model and AODV..................................... 84

14. Residual Error of the Analytical Model and DSR... 86

15. 5-Cube model versus Ad-hoc Network with Average Degree 4....................... 87

16. 5-Cube model versus Ad-hoc Network with Average Degree 6....................... 88

17. 5-Cube model versus Ad-hoc Network with Average Degree 8.......................90

18. 5-Cube model versus Ad-hoc Network with Average Degree 10......................91

19. Residual Differential of 5-Cube Model for AODV..92

20. Residual Differential of 5-Cube Model for DSR... 93

List of Tables

Table Page

1. Neighbor Hop Distance Frequencies for Hypercubes..50

2. Density of $C, 0 \leq c \leq 8$.. 61

3. Selected Factor Levels... 70

4. Selected Experiment and Simulation Parameters.. 71

A BLACK HOLE ATTACK MODEL FOR REACTIVE AD-HOC PROTOCOLS

I. Introduction

In the era of Net-Centric Warfare, warfighters utilize Command Control Communications Computers Intelligence Surveillance and Reconnaissance (C4ISR) systems to conduct distributed execution of missions throughout the theater of operation. These distributed components of the system are linked together by military networks to share information and provide dependable and resilient coordination, communication, and intelligence services to the warfighters. Military analysts consider this to be a force multiplier; fewer distributed and coordinating assets can outperform a larger opponent that executes centrally with little coordination [Fol11]. Moreover, the individual components performing distributed execution can become specialized to contribute to a particular part of the mission. While this has a desirable benefit, it places significant burden on the availability of the network. If the network becomes disrupted due to incorrect configuration, failures, or malicious activities the distributed components become isolated. The effect is that specialized units must act on local or outdated global information and may need to take on a larger burden of the mission, of which they may not be ideally equipped to address. Unless warfighters have access to secondary communication systems, they have no way to recover from this isolation and may quickly be consumed by the enemy. Thus, because of the use of Net-Centric Operations, the network becomes a critical resource to defend and a lucrative target to attack.

Because of the emerging importance of the network, the Joint Publication for Information Warfare JP 3-13 has defined Computer Network Attack (CNA) as an operation to attack enemy networks to minimize its availability (e.g., disrupt, deny, degrade) and Computer Network Defense (CND) to minimize the enemy's ability to degrade the United States military's access to its network [JP 3-13]. For both of these operations, it is important to understand the effects of availability attacks on multiple networks in the same way the effects of kinetic attack on structure is known. By knowing the effects of these attacks, the warfighter can study ways to circumvent threats against Air Force networks while planning effective attacks against the enemy's systems.

Availability attacks exist at every layer of the network stack for different types of network classes [BJJ07], [YaM03]. This thesis focuses on one availability attack at the network layer: the Black Hole attack for ad-hoc networks. Ad-hoc networks provide data routing services to loosely coordinating groups or quick reactionary forces, making it essential for current and future Net-Centric Operations. A Black Hole attack is a well-known denial of service availability attack for ad-hoc networks that deceptively attracts data to flow through nodes under control of an attacker. As packets of data flow into the malicious node, they are silently dropped. A highly successful Black Hole attack can prevent all data from reaching its destination. Therefore, this attack is a significant threat to Net-Centric Warfare because it causes isolation in this network.

While the Black Hole attack is well known, it has not been extensively studied. Of the existing research, most published work on Black Hole attacks involves measuring the effect of a Black Hole attack on protocols. However, there has been no research on the effectiveness of attacks on different instances of ad-hoc networks (e.g., different number of nodes, density, diameter). Moreover, there has been little research in understanding why the Black Hole attack is effective. One exception is work performed by Andre König, who developed an analytical Black Hole model to predict performance loss incurred by the network under attack [KSS09]. However, his model is limited to an optional configuration of a single mobile ad-hoc network (MANET) protocol. This thesis develops an analytical Black Hole attack model for ad-hoc topologies using reactive protocols that is complementary to König's work in that it is more general and is based on proven theorems.

1.1 Hypothesis and Goals

The hypothesis is: an analytical model can be used to predict the effect of Black Hole attacks on ad-hoc networks. To test this hypothesis, the results of an analytical model can be compared against the measured effect of a Black Hole attack in a controlled experiment. While previously developed analytical Black Hole models could be used in the experiment, there are several drawbacks to them that are covered in Section 2.3, which includes protocol applicability limitations and an incomplete model for how the Black Hole attracts new routes. One goal for this research effort is to develop a new analytical Black Hole model that overcomes the identified issues and provide an alternative method for assessing the impact of Black Hole attacks on networks. A secondary goal is to identify an alternative method to the uniform density assumption to simplify analysis on ad-hoc topologies.

1.2 Contributions

This thesis contributes in several ways. First, the performance constraints of a Black Hole attack are explored. From this exploration, a theorem is developed for reactive MANET protocols that select routes with the smallest hop-count during route discovery, on the existence of an upper-bound on the degree of deception a Black Hole can offer for its route advertisement. Assuming a Black Hole node will maximize its deceit to increase its chances as being selected for a route, an analytical model for Black Hole attack is developed based on this theorem that determines the probability that an arbitrary route in a network is subject to Black Hole packet dropping attack. The model requires the neighbor hop-distance density function be known for the topology. Since this function is unknown for ad-hoc topologies, the third contribution is the use of topology substitution to make the problem tractable. A hypercube topology with similar network properties is substituted for an ad-hoc topology to derive an approximate hop-distance density function. The fourth contribution is a method for finding the hop-distance density function for hypercubes given the network degree.

The academic impact of this contribution includes 1) greater understanding of the behavior of a Black Hole attack, 2) a new Black Hole attack model, and 3) an alternative topology approximation to the uniform density assumption to reduce the complexity of analysis for ad-hoc topologies. The military impact involves the duality of assessing the impact of a potential weapon of war. The military may utilize this model to evaluate the impact of Black Hole attacks on enemy systems for Computer Network Warfare. Conversely, the military may also use the model to determine the susceptibility of Black Hole attacks on their systems and explore alternative network designs that minimize the risk.

1.3 Structure of the Thesis

The remainder of this thesis is organized into six chapters. Chapter II provides background material on ad-hoc networks, Black Hole attacks, and analytical models for Black Hole attacks. Chapter III supplements the background research with a new theory for Black Hole attacks and ad-hoc topology approximation using hypercubes. The two concepts are combined in this chapter to present a new analytical Black Hole attack model for hypercube topologies. Chapter IV provides the methodology for establishing an experiment to test the accuracy of the analytical Black Hole attack model on ad-hoc topologies. Chapter V presents and provides analysis of the results of the experiment. Chapter VI summarizes the accomplishments, conclusions, and future work of this thesis.

II. Literature Review

This chapter covers background material and prior work related to this research effort. The chapter is structured as follows: Section 2.1 contains background material on ad-hoc networks, a generalized architecture of ad-hoc routing, and two reactive routing protocols that comply with the assumptions of the analytical model. Section 2.2 contains background information on the Black Hole network attack. In Section 2.3, existing research is presented on Black Hole performance analysis using simulation, ad-hoc topology approximations for analytical models, and two analytical Black Hole attack models.

2.1 Ad-Hoc Networks and Routing

An ad-hoc routing service is comprised of four core components: 1) determining topology state, 2) calculating routes, 3) selecting a route, and 4) forwarding packets according to the selected route. The relationship between these components is shown in Figure 1 [ZPY10]. The architecture represents the functions of the protocol as a system and therefore is not bound to the physical manifestation of a network. This means that one node may contain all or some of the component functions or merely participate as a single component. When combined, the protocol components provide two essential services. First, *Protocol Coordination* provides control of the *Path Information Base*, which is a data structure that holds current routing rules and policy. Second, *Application Routing* uses the *Path Information*

Base to route packets through the network. The services provide a control and data channel respectively.

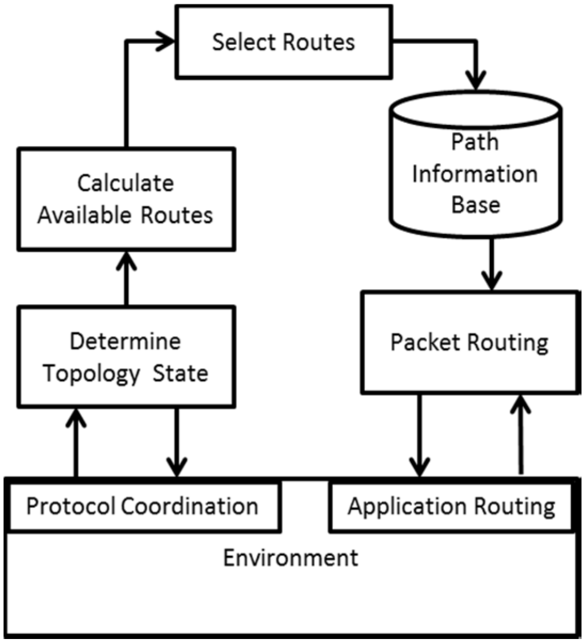

Figure 1: Ad-hoc Routing Protocol Architecture. Adapted from [ZPY 10]

The predominant challenge for the *Protocol Coordination Service* is to realize and maintain the state of network topology while contending with confounding dynamics in the physical, RF, and logical domains. Examples of dynamic events include node power failures, RF interference, and topology discovery on initial deployment. Global awareness of these events is achieved through protocol coordination, through which participants discover and exchange local topology state with peers to identify potential routes. During the *Calculate Available Routes* phase, feasible routes are realized using the updated topology state. In the *Select Routes* phase, the best route or routes (i.e., for multicast) are selected according to the particular route metric specified in the protocol. This subset of routes is stored in the *Path Information Base* data structure (e.g., cache, routing table, etc.). The *Packet Routing* component provides the second service, *Application Routing*, which routes packets according to the current rules and policies in the *Path Information Base*. Thus, as the state of the *Path Information Base* changes, the routing behavior of the network will change.

Ad-hoc routing protocols can be described in terms of five cross-cutting aspects over the architecture [OYM02]. These are 1) *Routing Time*, 2) *Routing Direction*, 3) *Information Placement*, 4) *Routing Structure*, and 5) *Alternative Route*, where each aspect has at least two alternatives. For the *Routing Time* aspect, protocols can be proactive or reactive in how they maintain topology state through coordination. Reactive protocols only coordinate when necessary, while proactive protocols coordinate periodically. The tradeoff between reactive and proactive is between route setup time and bandwidth. Proactive protocols have more deterministic route setup times at a cost of utilizing higher bandwidth [FZJ09]. Reactive protocols utilize less bandwidth for control packets, but have higher variance in the route setup period [KiL07]. The aspect of *Routing Direction* describes the direction of a routing path with respect to the topology state dissemination direction (i.e., the direction that updated topology information travels with respect to the source node). Therefore, the route direction is either with or against the dissemination direction. The *Information Placement* aspect describes how the route is stored in the network. Traditionally this has involved storing the next hop in forwarding tables at each node making routing *hop-by-hop* or alternatively the source node is responsible for maintaining the complete route. The

Route Structure aspect describes whether the protocol assumes that all nodes do the same work (i.e., flat) or that there is a hierarchy of roles. Finally, the *Alternative Route* aspect describes whether the protocol supports single-path or multipath packet routing.

2.1.1 Ad-hoc On-demand Distance Vector Routing

Ad-hoc On-demand Distance Vector (AODV) routing is a reactive routing, forward updating, hop-by-hop, flat, and single-path routing protocol [PBD03]. The protocol is broken into three services: 1) Route Discovery, 2) Route Repair, and 3) Packet Forwarding. The Route Discovery process occurs when a source node desires to route to a destination. The source node sends a route request (RREQ) packet that is flooded throughout the network via broadcast. To minimize the effects of broadcast collisions, each node waits a random interval before initiating its broadcast of the RREQ. As the RREQ is propagating the network, intermediate nodes append their ID to the RREQ and store a forwarding rule towards the source in preparation of a reply message. When the destination, or an intermediate node that knows the forwarding path to the destination, receives a RREQ it responds with a route reply message (RREP). The responding node places the path information collected during the RREQ into the RREP and sends it along the reverse path previously established during the RREQ flood to the source node. Each node that receives the RREP adds the forwarding rule to their route table and forward the RREP toward the source. Because of the flooding nature of a RREQ, the destination generates a RREP for each discovered path.

Route Repair consists of a detection event and response. Along a forwarding path from a source to a destination, the transmitting node expects an acknowledgement packet for each forwarded packet. If the node receiving the packet fails to respond, it may retry several times. Upon repeat failures a route error (RERR) packet is generated along the reverse route of the failed packet back to the originating source node of the packet. Each node that receives the RERR packet marks the forwarding rule pertaining to the broken route as having an infinite hop distance to the destination. Upon receiving the forwarded RRER packet, the source node attempts to repair the route by initiating a new RREQ packet.

Intermediate and source nodes receiving a RREQ, RREP, or RERR update their forwarding table if 1) the destination's sequence number in the coordination message is higher than the one stored in their table, or 2) the destination's sequence number is the same as the entry in its routing table, but the hop-count in the message is shorter. Coordination messages containing higher destination sequence numbers imply fresher routing information.

Sequence numbers are an important part of updating the topology. Each node is responsible for maintaining the current value of its own sequence number. A node updates its sequence number upon generating either a RREQ or RREP. It places the new sequence number in the source sequence field for a RREQ and the destination sequence number field for a RREP. These two events describe the majority of destination sequence updates for a network; however, there is a special case where an intermediate node increments its local copy of a destination's sequence number. This happens when a node detects a link failure and subsequent

RERR message. The updated destination sequence number is included in the RERR message and since it is greater than the last known true destination sequence number, causes each downstream node to update its table before forwarding the RERR down the reverse path to the source. The two independent sequence numbers represent the partition in the route, which is only corrected by the source node instigating another RREQ. If the destination receives the new RREQ and sends a RREP, the resulting sequence number will always be equal or greater than the sequence number generated by the original sender of the RERR. For the nodes that update their tables based on the RERR, if they receive a RREP with an equal destination sequence number they will still update their tables because any new and real route has a hop distance less than infinity.

Packet forwarding is achieved via a distance vector table stored at each node in the network containing entries for each known destination. For each destination, the node stores the next hop, distance in hops to the destination, and the sequence number of the latest update to the route. When application packets arrive to be forwarded, the node examines the destination in the packet and determines the next hop using the appropriate entry in the routing table.

2.1.2 Dynamic Source Routing

Dynamic Source Routing (DSR) is a reactive, forward updating, source-based, flat, and single-path routing protocol [JHM07]. Its route discovery and maintenance behavior is very similar to AODV; however, the major differences between the protocols are the manner of packet routing and how the routes are stored. Unlike

AODV, the route is maintained completely by the source node in DSR. The source node is responsible for generating the route request and has complete freedom to select any route reply to use when routing packets. Instead of storing the route hop-by-hop, DSR uses source routing where the source node places complete routing information in each application packet. Each intermediate node along a route will use this information to determine the next hop. The intent of the designers is to follow the analog of the TCP/IP fate sharing [Cla88] by placing the majority of the complexity burden at the end nodes. With route selection at the end nodes (i.e., the source and destination nodes), inner nodes (i.e., the nodes that forward packets along the route between the source and destination) can be stateless. This removes any need for inner node router memory [JHM07]. However, if all nodes fully implement DSR, the protocol uses route caching to minimize delay in learning a new route. Nodes cache routes from 1) route responses to route requests, 2) source routes that have traversed through the node, and 3) overheard control messages from neighbors. Upon receiving a route request packet that is requesting a route to another node, the intermediate node consults its cache to determine if they already know a route. If a route is found in its cache then it generates a route reply rather than continue flooding the original route request message. Similar to AODV, before broadcasting a RREQ, a node will wait a random amount of time to minimize that chance of a collision during broadcast.

The route discovery process in DSR enables the source node to realize and cache multiple paths to a destination. If the source receives a route error message on one of its routes, it can look in its cache to determine if an alternative route is already known. The *Route Selection* function in DSR is not defined in [JHM07], but rather, is left up to the implementation of the protocol. The DSR simulation model in ns-2.34 [Net11] selects the route in the cache with the smallest hop count. In picoNet [Son09], a Linux 2.4 Kernel module implementation of DSR, the shortest hop count route is selected from the route cache. During a tie, the most current route entry of the shortest routes is selected. The Monarch Project implementation of DSR for FreeBSD3.3 also selects the route in the cache with the lowest hop-count [Ric00]. All of these implementations select the route with the smallest hop-count.

2.1.3 Generalization of Reactive Protocols

One notable similarity with the majority of reactive routing protocols is the use of the route request and route reply exchange when establishing a new route. While DSR and AODV certainly do this, protocols such as Admission Control enabled On-demand Routing [KAD07] and Dynamic Manet On-demand Routing [ChP10] also utilize the route request flooding to find the destination followed by a route reply from the source. Moreover, many other reactive protocols such as ones proposed in [KGA06] and [GoY02] are extensions of AODV and DSR. These protocols provide minor improvements without significantly changing the *request-reply cycle*. Therefore, it is reasonable to assume the route discovery process in most reactive protocols exhibit the same behavior.

2.2 Black Hole Packet-Drop Attack

A Black Hole attack is a low-observable indiscriminant active packet-dropping attack [Lun00]. By silently dropping all received application packets intended for forwarding, a Black Hole packet-dropping node effectively denies end-to-end routing service for all routes traversing through it. To maximize its effectiveness, the packet-dropping node also participates in the coordination service of the routing protocol to coerce routes to include the packet-dropping node. The coercion process involves falsifying coordination data to make the Black Hole node appear as a lucrative and valid choice during route selection. Therefore, a Black Hole attack consists of two phases: 1) an attractor phase where coercion takes place and 2) an exploitation phase where packets are dropped from routes. The effect on ad-hoc routing protocols is shown in Figure 2.

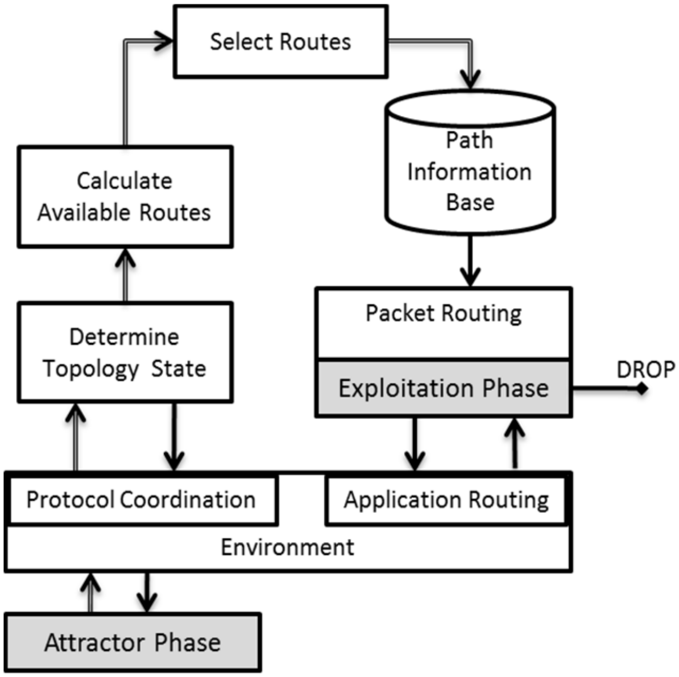

Figure 2: Black Hole Attack on Ad-hoc Routing Protocols

During the attractor phase, the goal of the attack is to get routes to flow through Black Hole nodes. This is accomplished by modifying the *Path Information Base* of the routing protocol, which is managed through the *Protocol Coordination* service. The path that this low integrity routing data takes during the attractor phase follows the double-lined arrows in Figure 2.

First, the attacker provides topology information so that the Black Hole node is perceived as being in at least one of the available routes, which is trivial. Through coordination messages, the attacker simply declares that there is a path between each targeted source and destination node pair and each path passes through the Black Hole node. For the purpose of calculating available routes, there is no difference whether the attacker indicates that the destination node is one hop or many hops away from the Black Hole; however, the information must be syntactically correct and not violate limits of the protocol. For example, DSR has a maximum source-route length because of the limitations of the DSR source route header size. A fabricated route that violates this limit would never be added to the *Path Information Base* and instead be silently dropped.

Second, the attacker must make it likely that at least one of the routes containing the Black Hole is selected as the route that goes into the *Path Information Base*. This critical part is handled during *route selection* and is protocol specific; however, many protocols use a routing metric to rank the fitness of each available route and select the fittest route to add to the *Path Information Base*. Examples of routing metrics include minimized hop count, maximized link quality over the route, maximized throughput, and minimized congestion. The particular routing metric used in a protocol can be design and implementation specific. DSR and AODV both use the shortest hop-count for route selection provided sequence numbers in the RREP message are correct.

There are several strategies for the attacker to offer a winning metric. First, the attacker can observe legitimate node coordination of topology information to learn the best metric the network can offer about a route. With this information the attacker can submit a route with a better metric that is guaranteed to be selected. However, it is not reasonable to assume that a node in a multi-hop network would always have complete visibility over all coordination messages in the network, so the attacker may not be able to learn the best route's metric. Instead, the attacker must estimate a good value from all available information.

A simpler approach for the attacker is to exploit known boundaries of digital systems and submit the best possible value for a metric. For example, the Black Hole attack in [DSE07] submitted the highest possible destination sequence number in a RREP to all route requests. According to the AODV protocol, topology information in a RREP replaces local table information if the destination's sequence number in the message is higher than the value stored in the nodes routing table. While this approach is simple and seemingly powerful, it still does not guarantee the Black Hole's route will be selected. There may be other available routes that coincidentally evaluate to the optimal value and thereby cause the protocol to defer to a secondary metric to break the tie. For AODV, the tie-breaking metric is to select the route with the shortest hop-count. Moreover, submitting the best possible metric value may be easily detected by more secure versions of the protocol. In

[DhS08], the authors used the fact that sequence numbers generally increase by small amounts and modified AODV to discard RREP messages with destination sequence number significantly larger than expected. Their analysis shows that this simple detection method avoided slightly less than half of Black Hole attacks. This result leads to an insight on the limitation of Black Hole forgery of topology information: Black Holes cannot lie with impunity. Instead, a stealthy Black Hole must balance the tradeoff of truth versus fiction by presenting fabricated, yet plausible, topology information that maximizes its utility during *Route Selection*. Black Hole constraints such as this are presented as new insights in Chapter III.

The exploitation phase commences once a route with the Black Hole node is included in the *Path Information Base.* This phase is very simple; the Black Hole conducts the denial of service attack on the route by dropping all packets instead of forwarding. What makes this exploitation particularly effective is that at this stage of the route the Black Hole node has the sole responsibility to provide feedback to the maintainers of the route that the packet was dropped. By silently dropping the packet the feedback loop is broken and downstream nodes will not be aware that packets are failing to arrive at the destination. Some protocols on top of routing such as TCP provide a built-in feedback mechanism [Ste94], but since a Black Hole node is between both the source and destination it can forge a reply as if from the destination (e.g., ACK) to complete the feedback loop.

2.3 Modeling and Simulation of Black Holes in Ad-hoc Networks

In this section, prior work related to the research topic is presented and evaluated. In Section 2.3.1, the limitations of existing performance analysis measurements of Black Hole attacks are identified. With respect to analytical modeling, existing ad-hoc topology approximations are summarized in Section 2.3.2 and two analytical Black Hole models are presented in Section 2.3.3. In these sections, the positive and negative aspects of the approaches are explored with the intent to guide the design for the analytical Black Hole model presented in Chapter III.

2.3.1 Research in Network Performance under Black Hole attack

The effect of Black Hole attacks on ad-hoc networks and MANET performance has been studied with controversy. In [CPZ09] and [BhS09], the DSR protocol is subjected to Black Hole attacks in simulation. Generally the results show a decrease in network throughput and packet delivery ratio as the number of Black Hole nodes increase. Studies of Black Hole attacks on AODV also show a similar trend in performance loss in [DSE07] and [KSS09]. One matter of concern is that performance results of independent studies on the same protocol are not consistent with each other. In König's study, two Black Hole nodes dropped 75% of all packets; however, Dokurer reports that two Black Holes dropped only 50% of the packets, which is well outside of König's confidence intervals. In Cai's study five Black Holes in a network reduced throughput by 30%; however in Bhalaji's study, throughput is reduced by 20% for the same number of Black Holes. Even more concerning is that these performance results were used to demonstrate the effectiveness of their approach in avoiding Black Hole attacks. Assuming these studies are not flawed, this implies that there is a relationship of Black Hole performance beyond protocol and number of Black Hole nodes.

2.3.2 Prior Research in Topology Approximations of Ad-hoc Topologies

Analytical models of ad-hoc networks involve topology assumptions to reduce analysis complexity of the topology graph. In [Bet02] the author uses network density

$$\rho = \frac{n}{A}, \tag{1}$$

to describe the topology, where *n* is the number of equal-distanced nodes placed in area *A*. This allows problems to be solved geometrically, such as 1) the minimum node degree of a graph, 2) the minimum transmission range so that no node is isolated, and 3) the expected degree of a network. The author identifies a discrepancy between simulation results and the analytical model. He argues that the error is a result of the assumption in the analytical model that there is no border; however, simulations such as ns-2 utilize a border to bound the area nodes can be deployed and move. The author suggests several ways to overcome the *border effects* in simulation including wrapping borders of the simulation to achieve a torus; however, adapting a simulation to fit an analytical model is counter-constructive. Assuming the simulation has been previously validated, it would be more beneficial that the un-validated analytical model be adapted to consider border effects.

Bettstetter used the same uniform density assumption in [BeE03] to derive the probability that two randomly selected nodes in a network are neighbors. The authors were also able to derive an analytical model for the probability that two nodes are exactly two hops apart; however, they were unable to find a closed form derivation for the general case, where H is a random variable of the hop-distance between two randomly selected nodes in a network. As a compromise, they provided statistical representation of the density function of H for hops greater than two. The paper includes several bar graphs depicting the density functions of H for a variety of network densities.

There is no published research using interconnection network topologies to approximate ad-hoc topologies. Interconnection networks have been used for organizing processing elements in super computers for efficient parallelization of complex tasks and their network properties are well studied [Hwa93]. This domain is far removed from wireless ad-hoc systems with dynamic topologies and limited resources, so this thesis is the first time that the application of both domains has been examined.

2.3.3 Prior Research in Analytical Black Hole Models

There are currently two analytical models for Black Hole attack in ad-hoc networks. The following sections describe the models, identify limitations, and suggest improvements to the models.

2.3.3.1 Aad's Denial of Service Attack Model

In [AHK08] an analytical model is presented to calculate network throughput under denial of service attacks; specifically these attacks are Jellyfish and Black Hole. Their model estimates the availability of a network flow (i.e., a group of packets traversing a route) based the proportion of time the flow incurs zero throughput. The expected time a route has zero throughput is calculated as the product of the probability that at least one malicious node is in an arbitrary route of a certain length and the expected correction time to expunge all malicious nodes from that route. The correction time is based on the number of attempts to detect the attack, rediscover an alternative route, and repair for each malicious node in the route. Given the expected interval of zero throughput, one can calculate availability as one minus the ratio of the time of zero throughput over the expected duration of the flow.

There are two concerns about this analytical model. First, the authors' simplification of the route setup process could introduce error. They assert that the probability a route h-hops in length has no malicious nodes is $(1-p)^h$, where p is the proportion of malicious nodes in the network. While they did not specify the probability distribution, this is a binomial experiment. Parameter h is the number of binomial trials and random variable X is the number of malicious nodes added to the route. The model is shown as a binomial distribution here

$$P(X=0)=\binom{h}{0}p^{0}(1-p)^{h-0}=(1-p)^{h} \tag{2}$$

If the authors assume route setup is truly binomial then they also must assert that node selection for each hop of the route is "identical and independent" [MiA03]. Assuming routing protocols are loop free, each trial is not identical or independent because once a node is selected for a route it should not be selected later in the route. Otherwise a routing loop has been introduced, which violates the common loop-free assumption of routing protocols. Each node selection during route construction changes p because malicious and benign nodes are removed from the sample pool and placed in the route. Since the authors' derivation assumes a binomial distribution, then there are issues with the model. A more appropriate distribution is the hypergeometric distribution which is used in König's model in Section 2.3.3.2.

Another concern regarding the manner of modeling route selection is that the effect of the attractor phase of a Black Hole attack is missing from the model. In the model, the probability that a Black Hole node is selected in a route is entirely based on the proportion of Black Holes in the network. While it is certainly intuitive that more malicious nodes increase the probability of selection, the model does not consider that a Black Hole will bias route selection so that it is more likely to be selected over other nodes. Instead, the authors' model assumes that the selection probability is divided equally for all nodes. These two shortcomings indicate that a simple Bernoulli experiment does completely explain the Black Hole attack effect.

The third concern is that the authors assume that detection of a Black Hole attack is a matter of eventuality. During the lifetime of a flow, any malicious nodes along the flow route will eventually be detected via 1) route diagnosis at the network layer, or 2) the use of the TCP feedback loop. Since a Black Hole node silently drops packets, the network layer will always be unaware of the broken route and would not know to issue a repair. Utilizing the transport layer instead of the network layer, the end-points of a TCP connection could measure throughput and terminate the route when throughput appears stalled. In theory this detects the effect of a Black Hole attack; however, the measuring mechanism in this case is also under the control of the malicious node. The proposed way for an endpoint to measure throughput is found in [CFG11], where the upper-bound of throughput is the maximum receive window size over the round-trip time (RTT). Since the malicious node is situated between the endpoints, it is reasonable to assume that the malicious node could provide spoofed acknowledgements on sent segments back to the sender to keep RTT estimates nominal. Given the normal RTT measurement, the connection appears to be working from the sender's perspective and the route remains persistent even though packets are actually being dropped.

While the authors' detection methods of Black Hole nodes could be avoided, there is an open question if Black Hole nodes are detectable. Several researchers propose detection methods revolving around a watch-dog system to monitor forwarding behavior to detect packet dropping, where the absence of forwarding implies packet dropping. Upstream nodes watch the downstream node to make sure they actually forward the packet in [TAC09] and [KHK09]. If they fail to forward several times they are blacklisted from participating in routes. However, in [AHK04], it is shown that watchdogs can be fooled if the Black Hole forwards the message to a bogus neighbor. An alternative detection method in [GAM07] detects the inconsistency between the falsified topology data presented by the Black Hole and the actual data for the Optimized Link State Routing (OLSR) protocol. They propose to distribute passive traffic sensors within the area of the network that detects local network traffic. This information is forwarded to a centralized anomaly detection algorithm for outlier detection and blacklisting. What is not clear is how the sensor network is immune from the same vulnerabilities as the MANET. For example, the centralized detector must trust the reports from external sensors, which could be forged or disabled by a man-in-the-middle attack.

The most promising approach to detect Black Hole nodes is to exploit the greedy nature of the Black Hole, where Black Holes desire to acquire many routes to maximize the network degradation effect. In [PSA09], routing agents bait potential Black Hole nodes by initiating route discovery on non-existent nodes. Normal nodes will not reply to a non-existing destination; however, a greedy Black Hole node will always reply. Therefore requesting routes to bogus destinations over the entire network will reveal Black Holes in the network.

For ad-hoc networks where nodes freely join or leave, it may be difficult to determine the set of bogus node IDs to use as lures. Moreover, the Black Hole node could observe network traffic to learn which nodes are real and only respond to future route requests about those nodes. While it is reasonable to assume that more advanced baiting schemes could be used to find Black Holes, it is also reasonable to assume that more complex Black Hole attacks can be developed to hide from detection. Therefore, the problem of detecting Black Holes remains to be solved.

2.3.3.2 König's Black Hole Attack Model

A completely different Black Hole model is proposed in [KSS09] to model packet loss instead of throughput of an AODV MANET under a Black Hole attack. Like Bettstetter, König assumes uniform node density to simplify the topology to determine the number of nodes included in a given topology search area. By letting the radius of this search area be a multiple of the transmission distance, one can geometrically determine the number of nodes reachable at each hop. In addition, the search area factors in border effects. While this addresses the problem Betstetter encountered with the uniform density assumption, the authors acknowledge that their method is not completely sufficient to describe the effects of borders on the route discovery process.

Given the ability to estimate the number of nodes at each transmission hop, they model the optional AODV RREQ extension known as the expanding ring topology search. The expanding ring search is an AODV extension that avoids the potential for wasted forwarding of RREQ messages beyond the destination in the base protocol. The source node accomplishes this by iteratively sending out RREQ messages, where each iteration uses a higher time-to-live (TTL) value. The source node starts with all one-hop neighbors and increases the TTL value on subsequent

RREQ messages until the destination is discovered or the expected end of the network is reached.

Given the set of nodes included in the i^{th} RREQ of the expanding ring search, König can find 1) the probability that at least one Black Hole and 2) the probability that the destination is within the search area. The first probability is defined as

$$p_{black}(i) = \begin{cases} 1 & if\ n_i > n_{total} - n_{black} \\ 1 - \frac{\binom{n_{total}-n_{black}}{n_i}}{\binom{n_{total}}{n_i}} & otherwise \end{cases} \tag{3}$$

where n_i is the total number of nodes that the RREQ traverses in the i^{th} RREQ of the ring search. There are n_{total} number of nodes in the network and n_{black}Black Hole nodes. Unless the RREQ has reached all benign nodes in the network, the probability that at least one Black Hole gets a RREQ in the i^{th} ring search is the probability that $n_i$does not contain all benign nodes. This is the opposite of the probability that $n_i$is completely comprised of benign nodes, which is simply the ratio of all possible benign selection events and all possible combinations of selection events.

The second probability $p_{dest(i)}$ is the number of new nodes (i.e., $n_i - n_{i-1}$) reached in the i^{th} RREQ over n_{total}. This is intuitive considering that while the i^{th} search reaches n_i nodes, n_{i-1} have already been explored in previous ring search iterations and did not find the destination.

König asserts that the probability an arbitrary route is subject to a Black Hole attack is the summation of the conjunction of $p_{dest(i)}$ and $p_{black(i)}$ for each iteration of the expanded ring search. This is:

$$p_{loss} = \sum_{i=0} p_{dest(i)} \cdot p_{black(i),\ n_i \leq n_{total}} \tag{4}$$

There are several observations to note about the important work in [KSS09]. First, the authors implicitly include the condition for a Black Hole to win a route in the expanded form of (4). For the i^{th} RREQ, the route is subject to Black Hole attack if there is at least one Black Hole in n_i and the destination node is one of the new nodes reached during the iteration. In this model, a Black Hole contaminates the *Path Information Base* in response to a $RREQ_{s,d}$ from source *s* to destination *d* if there is at least one Black Hole with a hop count distance to the source node that is less than or equal to the hop count between the source and destination. While the authors do not explicitly identify this, it is intuitive when considering route selection of AODV. Nodes that are closer to the source may respond faster to the source [DSE07], or more importantly, may be more likely to have a better routing metric (i.e., hop count) than the destination. A Black Hole replying with a better metric than the destination will be selected instead of the destination. Consequently, the Black Hole's solicitation is added to the *Path Information Base*. This condition is formalized as a theorem in Chapter III.

Secondly, the authors either did not realize or convey that the expanding ring search sequence is very similar to the standard route request flooding process in AODV and DSR, which would greatly enhance the scope of their analytical model.

Because the distance to the destination is probabilistic in (4), the analytical model considers all possible hop distances to the destination. For this reason, (4) could also model a single standard RREQ message that is flooded throughout the network when the distance to the destination is probabilistic. Before the model can be applied, some assumptions have to be made. First, instead of iterations, there are steps within the discovery process. Each step represents the state of a single RREQ flood having reached all neighbors *s*-hops away from the source. At the beginning of the step *s*, $\Delta n = n_s - n_{s-1}$ receive a forwarded RREQ message [KSS09]. Each node in Δn processes and synchronously forwards the RREQ for step *s+1*. By assuming each step is synchronized and forcing the step value to be incremented by one for each step, the calculation of n_s is the same as n_i for the expanding ring search. A second assumption is that the reduction in the number of RREQ messages for the base AODV does not invalidate the model. Given that König's model does not consider temporal or bandwidth constraints, then substituting one RREQ for the multiple RREQ in the expanding ring search should not be an issue. Given these assumptions, their model may be applied to model the standard route discovery process for AODV and DSR.

The third insight into König's analytical model is that the number of Black Holes in n_i is actually a hypergeometric random variable and is equivalent to the calculation of $p_{black}(i)$ when $n_i \leq n_{total}$ - n_{black}. Let B be a hypergeometric random variable for the number of Black Holes less than or equal to i hops from the source. In terms of a hypergeometric problem, let n_{total} be the population size, n_i be the sample size, and n_{black} be the proportion of the population with the desired trait.

The probability that there are exactly b Black-Holes closer than the destination to the source is:

$$P[B=b]=\frac{\binom{n_{black}}{b}\binom{n_{total}-n_{black}}{n_i-b}}{\binom{n_{total}}{n_i}} \tag{5}$$

Only one Black Hole is necessary to win a route and begin dropping packets. If two Black Hole nodes ended up in the same route only one of them would actually drop the packets. Let $P[B\geq 1]$ be the probability that at least one Black Hole is in the n_i nodes reached in the ith RREQ. By the axioms of probability this is equivalent to $1-P[B=0]$. Substituting $b=0$ into (5) results in the derivation of (3), which reveals that König's model is hypergeometric:

$$1-P[B=0]=1-\frac{\binom{n_{black}}{0}\binom{n_{total}-n_{black}}{n_i-0}}{\binom{n_{total}}{n_i}}=1-\frac{\binom{n_{total}-n_{black}}{n_i}}{\binom{n_{total}}{n_i}}, n_i\leq n_{total}-n_{black} \tag{6}$$

III. Analytical Model for Black Hole Attacks

This chapter describes an analytical model to determine the effect of a Black Hole attack on a wireless ad-hoc network given a minimal set of parameters to describe the intensity of the attack on a network topology.

The remaining sections in this chapter are organized as follows. Section 3.1 describes the assumptions that must hold for the model to produce valid results. Section 3.2 identifies the objectives and constraints of Black Hole attacks. These limitations lead to the formulation of a generalized predicate that describes the condition when a Black Hole attack is successful, which is covered in Section 3.3. Unfortunately, the predicate requires *a-priori* knowledge about the relative positions of nodes in the network which makes evaluating the predicate against ad-hoc topologies difficult. Section 3.4 presents a solution to this problem by using a hypercube topology as an approximation to an ad-hoc topology. The benefits and drawbacks of this approximation are described, and more importantly, a method for deriving the neighbor hop-distance density function for hypercubes is presented. Section 3.5 describes an analytical model for determining the probability a Black Hole node in a network successfully attracts an arbitrary route. Section 3.6 reveals a simple model for determining the performance impact of Black Hole nodes deployed in a network by utilizing the attractor model from Section 3.4.

3.1 Analytical Model Assumptions

This section declares assumptions made about the ad-hoc network for the analytical model. They describe the assumed behavior of the topology, protocol, benign (i.e., non-malicious) nodes, and Black Hole nodes. Because the analytical model is based on these assumptions, they bound the scope of this research.

3.1.1 Topology Assumptions

- The average node degree of the network is known *a-priori*.
- Nodes are never added nor removed from the network.
- The operating area is square and is fixed in surface area and origin.
- Every node in the network has at least one neighbor (i.e., the network is not partitioned).
- The nodes in an ad-hoc network are randomly placed in an area using uniformly random variables for each dimension.

3.1.2 Protocol Assumptions

- The ad-hoc network is using a reactive route protocol with a RREQ-RREP cycle for topology discovery and update.
- Route selection selects the route with the lowest hop count.
- Each node in the network will receive every RREQ message.

3.1.3 Benign Node Behavior Assumptions

- All benign (i.e., non-malicious) nodes have equal probability of initiating a RREQ message to a randomly selected destination over the lifetime of the network.

- Benign nodes are unable to discriminate between other benign and Black Hole nodes. Therefore, Black Hole nodes are treated as a normal protocol-compliant and trusted nodes by all benign nodes in the network.
- The destination node is the only benign node that replies to a RREQ. This implies that no intermediate nodes provide replies from their local *Path Information Base*.

3.1.4 Black Hole Node Behavior Assumptions

- A Black Hole can predict and match the destination sequence number in a destination's RREP in AODV.
- A Black Hole node will always reply to a RREQ with a forged route.
- A Black Hole node will drop all forwarded packets.
- Black Hole nodes do not collude and are never a source or destination.

3.2 Optimization of Black Hole Attacks for Reactive Protocols

A Black Hole node cannot act with impunity in the network. Instead, it is bound by what it wants to do versus what it is able to achieve. This section explores the impact that constraints such as protocol, locality, topology, and physical have on the success of a Black Hole attack. The objectives and constraints are used to bound the design of the analytical model. While not all constraints are considered in the model, they are included below for completeness.

3.2.1 Objectives of a Black Hole Attack

The effective performance degradation of an ad-hoc network under Black Hole attack is based on how many routes the attacker can influence and the length of time these routes remain in the *Path Information Base*. To maximize these values, the Black Hole must 1) respond to every possible RREQ, and 2) avoid behavior that prematurely ends a route's lifetime. If a Black Hole does not respond to a particular RREQ, then it has no chance of corrupting that route and it is blatantly in violation of the maximization objective. Once a route has been corrupted, the Black Hole must avoid being detected, causing a routing error, or providing insufficient feedback to the source at higher layers of the protocol stack (e.g., TCP). Any of these behaviors could cause the route to be torn down before the source was finished, minimizing the number of packets the Black Hole could have dropped. Therefore, a Black Hole maximizes the number of routes it influences by responding to every RREQ packet and maximizes the route's lifetime by being stealthy.

3.2.2 Limitations on Receiving RREQ Messages

The attacker must be able to participate in the *Protocol Coordination* service in order to have the opportunity to affect the availability of a network. For reactive protocols, a Black Hole node must be aware that a route discovery instance has commenced. This occurs when a Black Hole node receives a RREQ, but this is not guaranteed to happen. Both AODV and DSR have built-in mechanisms to shorten the route setup time, which limits the extent that route requests are propagated. The conditions where a Black Hole may not receive a RREQ are listed below:

1. A destination node never forwards a RREQ. Instead it generates a reply when the RREQ is unique. If a Black Hole node is in a position

where all paths to the source node pass through the destination, it will never receive an RREQ and the attack will fail against that particular route.

2. AODV and DSR permit intermediate nodes to respond to a RREQ if they have a fresh answer in their cache or routing table. The effect of a *cache hit* creates the same condition as the destination node. If the Black Hole node is in a position where all paths to the source node pass through an intermediate node that incurs a cache hit, then the Black Hole node is prevented from receiving a RREQ message for that route.
3. A ring search is used to limit the extent the route request is flooded. The search distance is controlled by the time to live (TTL) field in the IP header. Starting at TTL=1, the source node can determine if any neighbors exactly one hop away have a route to the destination. If this does not result in a route discovery, then the TTL is incremented and the search is repeated. The search distance is monotonically increased until the route is discovered. If the destination node or an intermediate node with a cache hit is fewer hops from the destination than the Black Hole, then it is prevented from receiving an RREQ for the route.

The model ignores this constraint by assuming that every node receives a RREQ message. However, by Theorem 2 in Section 3.3, because the intermediate or destination node is in between the source and Black Hole in each of these three conditions, a Black Hole attack will not occur. This result is equivalent to the result that would occur if a Black Hole never receives the RREQ message.

3.2.3 Limitations on Protocol Compliance

While the attacker can elicit behavior that is not protocol compliant, coordination messages must be protocol compliant to avoid being discarded by legitimate nodes. Depending on the protocol, the Black Hole node must also submit correct contextual state data often in the form of sequence numbers so that the coordination messages are accepted by benign peers. DSR and AODV use source sequence numbers to discriminate between different route discovery instances. If a recipient receives a RREP with an incorrect source sequence number, it will silently discard the packet.

Additionally, distance sequence vector protocols like AODV and DSDV use a destination sequence number as a quality of freshness in the topology updates (i.e., RREP). Since a node will not accept a new coordination message from a peer if the sequence number in the message is lower than the sequence number it has stored from a previously accepted coordination message, a Black Hole node must learn, deduce, or predict correct sequence numbers to successfully coordinate with peers during the routing process.

For example, a Black Hole can learn current destination sequence numbers of each peer by periodically attempting to establish a connection with each one of them. Each discovery process reveals the sequence numbers of the peer, which can be stored in a local repository for later mischief. Additionally, this repository of sequence numbers can be maintained by eavesdropping on control packets of route discovery processes of neighbors. In [KHK09], König suggests simply counting the number of overheard RREQ messages from each node and placing that value in the forged RREP; however, this assumes that the Black Hole gets all RREQ about a destination. While neither of these approaches guarantee the Black Hole has clairvoyance on the precise state of each potential destination, it will be able to estimate of destination sequence numbers that likely meet or exceed the true value without appearing excessive to anomaly detection methods such as those found in [DhS08].

The model developed in this thesis assumes that, for AODV, the destination's sequence number is known by the Black Hole node and it provides a matching sequence number in its RREP to force route selection to be based on hop count. This allows AODV behavior to match the *Route Selection* process in DSR.

3.2.4 Availability Limitations on the Packet-Dropping Attack

Ideally, the best a Black Hole node can achieve is to be included in every route that exists within a network. However, a Black Hole node is subject to the same physical constraints (e.g., bandwidth, medium contention) as any other node. Therefore it may be physically impossible to achieve complete domination of the network because of self-imposed congestion.

As a greedy Black Hole attracts more routes through itself, congestion at and around the Black Hole will increase. Eventually the Black Hole node and surrounding neighbors will be unable to service packets at a rate exceeding the arrival rate due to increased contention for the wireless medium. As a result, their send queues will fill up and packets will incur excessive routing delays. Worse, the delays could be so extreme that a node is unable to acknowledge receipt of a received packet causing a RERR to be generated and the Black Hole to lose control of a route under its dominion.

Both localized congestion and RERRs leak information to other nodes that could be used to detect the presence of a Black Hole. Moreover, the Black Hole node will have increased difficulty participating in coordination of new routes because coordination messages will be delayed or dropped in trying to traverse the congested region around the Black Hole node. Ironically, an overly greedy and successful Black Hole node may actually perform a denial of service attack on itself. By denying itself the ability to attract new routes, a Black Hole is unable to achieve the maximum theoretical effect described in Section 3.2.1.

An attacker may mitigate the bottlenecking of traffic of a single Black Hole by deploying multiple Black Hole nodes throughout the network. The drawback to this strategy is the attack complexity increases: it is more difficult to access a network, discreetly coordinate when necessary, and conceal the presence of a wide scale attack. On the other hand, an increased presence of greedy Black Hole nodes means more chances for the attacker to bid on each route request.

This model does not consider throughput limitations of Black Hole nodes. Instead, it permits the analysis of effect of multiple Black Hole nodes and assumes there is no upper limit to throughput for each Black Hole.

3.2.5 Limitations of Falsification in Coordination Messages

For protocols such as AODV and DSR that select the route with the shortest hop-count, a Black Hole must fabricate the shortest hop-count route possible to maximize the chance its route is selected. This section defines the shortest route a Black Hole can advertise that, if selected, will result in a packet dropping attack.

Lemma 1: *To conduct a packet-dropping attack, a Black Hole node must advertise correct topology state data about the path between the source node and itself.*

Proof. Assume a Black Hole node submits false topology state data in a RREP. In particular, the segment of the route between the source and the Black Hole does not reflect the true state of the topology. Assume that the source selects the route advertised by the Black Hole and begins forwarding packets to the destination. Since the segment between the source and Black Hole is false, packets will never arrive at the Black Hole. If packets never arrive at the Black Hole, then they cannot be silently dropped. Therefore, submitting an incorrect path between the source and Black Hole does not cause packets to be dropped. By contrapositive, a Black Hole must submit correct topology state information between itself and the source node to be able to conduct a packet-dropping attack.

Moreover, any protocol-compliant nodes along the forwarding path, including the source, before the Black Hole will identify the false path as a broken route and begin repairing or tearing it down. This causes the route to be removed from the *Path Information Base* and consequently results in a reduced disruption effect.

While it could be argued that repeatedly causing routes to fail and be recalculated is a denial of service and energy depletion attack, it is not stealthy and is not a packet-dropping attack.

Lemma 2: *To conduct a packet-dropping attack, the advertised segment between the Black Hole node and the destination must start with the Black Hole node and end with the destination; however, any arbitrary path can be placed between these nodes.*

Proof. Assume Lemma 1 holds and all routes are loop-free. Assume a Black Hole node submits arbitrary topology state data in a RREP. If the segment between the Black Hole and destination does not start with the Black Hole, then because of the loop-free assumption, the segment of the route between the source and Black Hole also does not end with the Black Hole. This violates Lemma 1, implying that a packet-dropping attack is impossible. If the segment between the Black Hole and destination does not end with the destination, then the source will not select the route because the response to its RREQ failed to satisfy its routing query of a route to a given destination. If it does not select the Black Hole's route, a packet-dropping attack will never occur. Finally, any arbitrary routing path can be placed between the Black Hole and the destination in the advertised route because the packet will be dropped by the Black Hole node before it is forwarded over the false section of the route.

Theorem 1: *The shortest path a Black Hole can solicit resulting in a packet-dropping attack is the shortest path between the source and Black Hole plus one.*

Proof. Assume Lemma 1 and 2 are true. By Lemma 1 the path between the source and Black Hole must be correct, so the minimal path length of this segment is the shortest legitimate path between the source and Black Hole. By Lemma 2, the path between the Black Hole and destination can be anything so long as it begins and ends with the Black Hole and destination. The shortest route that satisfies this is when the Black Hole advertises that the destination is a one-hop neighbor. Therefore the minimum advertised path length for this segment is one hop. When the two segments are combined, the shortest path that a Black Hole can advertise is the shortest real path between the source and Black Hole plus one hop to the destination.

3.3 Black Hole Attack Predicate for Route Selection by Hop Count Metric

Let N be the set of all nodes in an arbitrary ad-hoc network. Let B be a set of Black Hole nodes, where $\mathrm{B} \subset \mathrm{N}$. Let E be the subset of benign source, destination, or forwarding nodes in the network. Let $\mathrm{E} \subset \mathrm{N}$ and $\mathrm{E} \cap \mathrm{B} = \{\emptyset\}$. Let $\mathrm{RREQ}_{\mathrm{s,d,i}}$ represent the i^{th} route request from source node $\mathrm{s} \in \mathrm{E}$ about a route to destination node $\mathrm{d} \in \mathrm{E}$. Let κ be the number of unique real paths from s to d. Assume $\mathrm{RREQ}_{\mathrm{s,d,i}}$ reaches every node in N and there is no caching by intermediate nodes. Consequently, the source will receive κ RREP messages from the destination and one RREP message from every Black Hole in B. Let set RB with cardinality $|B|$ contain only Black Hole RREP messages. Let set RE with cardinality κ, $R\mathrm{E} \cap \mathrm{RB} = \{\emptyset\}$, contain legitimate responses from d.

Lemma 3: If there is a least one Black Hole where the distance to the source node plus one hop is less than the distance between the source and destination, then a route between the source and destination will be subject to Black Hole attack.

Proof. Assume Theorem 1 is true. Let $\min_{hc}(X)$ be a function that returns the minimum hop count from a set of RREP messages. From the implementation of DSR and AODV, route selection selects the RREP with the lowest hop count. Therefore, a route will be subject to Black Hole packet drop attack if:

$$min_{hc}(RB) < min_{hc}(RE) \tag{7}$$

If a RREP in RB exists that has a lower hop count than the shortest legitimate route from s to d, the Black Hole's route will be selected. Let $h(x, y)$ be a function that returns the minimum hop distance between arbitrary nodes x and y. The shortest legitimate path from the source to the destination is the route in RE with the minimum hop count, or $min_{hc}(RE) = h(s, d)$. From Theorem 1, the shortest path a Black Hole can solicit is the shortest path between the source and Black Hole plus one hop, or $h(s, b) + 1$. A route will be subject to Black Hole attack if at least one Black Hole's minimal route is shorter than the shortest distance between the source and destination. That is,

$$\exists b \in B[\, h(s, b) + 1 < h(s, d)] \rightarrow BlackHole\ Attack \tag{8}$$

Lemma 4: Consider the special case where predicate in (8) is false but there exists a Black Hole whose distance to the source node plus one hop is equal to the shortest path between the source and destination. For this case, a route from the source to the destination will be subject to Black Hole Attack.

Proof. Assume $\exists b \in B[\, h(s,b) + 1 = h(s,d)]$ is true. By design and implementation of AODV and DSR, when two RREPs arrive with the minimum hop count, the first RREP to arrive is selected. Since hop count is a non-negative integer, if $\exists b \in B[\, h(s,b) + 1 = h(s,d)]$ is true then $\exists b \in B[\, h(s,b) < h(s,d)]$ is also true. This implies that if the shortest route solicited by a Black Hole is equal to the shortest path between the source and destination, then the Black Hole node is closer to the source than the destination is to the source. Assuming homogeneous congestion throughout the network, no route caching by inner nodes, and ignoring the effects of random delays incurred at each node to minimize broadcast collisions, a route reply sent by Black Hole b will arrive before the destination node's route reply because the Black Hole has fewer hops to traverse than the destination. Since the Black Hole's RREP arrives first, its route will be selected over the legitimate route.

Theorem 2: *A route from a source to a destination will be subject to Black Hole attack if the Black Hole is closer to the source node than the destination to the source. That is*

$$\exists b \in B[\, h(s,b) < h(s,d)] \rightarrow Black\ Hole\ Attack \tag{9}$$

Proof. By combining Lemma 3 and 4, a route is subject to Black Hole attack if $\exists b \in B[\, h(s,b) + 1 \leq h(s,d)]$. Since hop count is a positive integer, if this predicate is true then $\exists b \in B[\, h(s,b) < h(s,d)]$ is also true.

This predicate identifies that a Black Hole's ability to corrupt routes is based on its relative locality with respect to the source and destination. If the Black Hole is closer to the source than the destination, it will corrupt a route. While this is elegant, it introduces a challenge of determining the relative hop distances between the source, destination, and each Black Hole node in the network. Given that the topology and positions of each Black Hole is known, each possible source-destination combination can be evaluated on its susceptibility against a Black Hole using the predicate in (9). In this case, the probability of attack is the total number of source-destination pairs where the predicate is true, over the total number of possible source-destination pairs. Assuming each route has equal traffic load, then this is also the expected portion of network traffic dropped due to Black Hole attack.

Unfortunately, the purpose of an ad-hoc network limits the feasibility of knowing the topology state *a-priori*; however, the constraints of knowing the exact relative distances of a particular topology could be relaxed. In this case, the relative distances between neighbors can be represented by a probability distribution. Given this information, the probability the predicate in (9) is true can be calculated.

The derivation of the probability density function of the relative hop-distances between neighbors for ad-hoc topologies has not been achieved. While the derivation has been attempted without success in [BeE03], the author instead elects to derive the distribution statistically by sampling randomly generated ad-hoc topologies with similar properties as the target network. While this approach is reasonable for high-fidelity calculations, it may be excessive for low-fidelity calculations. To keep analysis in the theoretical domain, an alternative approach that this thesis is proposing is to find a theoretical network topology where 1) the probability density function for relative hop-distances can be calculated, and 2) its structure is similar to an ad-hoc network topology. Given these conditions, the hop-distance density function of the theoretical topology can be substituted as the density function of an ad-hoc network of similar properties. This substitution allows (9) to be approximated probabilistically for ad-hoc networks.

3.4 The Hypercube Topology Approximation for Ad-Hoc Topologies

This research assumes that a hypercube is a good representation for ad-hoc topologies with the same average node degree because 1) the neighbor hop-distance can be derived, and 2) the density function is close to the statistical results in [BeE03]. The properties of a hypercube (a.k.a., binary n-cube) are well known and presented in [SaS88] and [Hwa93]. While there are other potential candidates for topology substitution, such as a *k-ary n-cube*, *torus*, or *n-ary tree*, exploration of these topologies is left as future work.

The remaining sub-sections of Section 3.4 are as follows. Section 3.4.1 and 3.4.2 describe the benefits and drawbacks of applying this topology to approximate an ad-hoc topology. Section 3.4.3 describes a hop count frequency function for hypercube topologies. This is used to find the probability that a neighbor is h-hops from a reference node.

3.4.1 Benefits of Hypercube Topology Approximation

The primary benefit for using a hypercube approximation is that the approximation makes the problem of finding the probabilistic distances between the source, destination, and Black Holes computable. The following paragraphs in this section elucidate the specific benefits.

First, a hypercube can compactly be described by *n*, which is the node degree at each node. When mapping from ad-hoc topologies to a hypercube, the average node degree is the only information required to generate a hypercube approximation of the ad-hoc topology. This simplifies the effort of characterizing the parameters of the ad-hoc network under study.

Second, hypercubes are symmetric, which reduces the complexity of the analysis with respect to a reference node. Ignoring the identities of each node, the perspective of the topology from any particular node is no different than any other node. This permits the analysis from a single arbitrary source node (a.k.a. *reference node*) to apply to any possible source node in the hypercube. Instead of evaluating (9) for all possible source-destination pairs, (9) is evaluated for a single *reference node* against all possible destinations.

Third, since the topology is well-defined, the probability that nodes are h-hops away can be computed. This precisely solves the issue presented in Section 3.3. With the probabilities for neighbors being h-hops away, the relative positions between a source, the Black Hole nodes, and the destination can be evaluated. The method for deriving the hop distance density function is described in Section 3.4.3.

3.4.2 Drawbacks of Hypercube Topology Approximation

Because the hypercube is approximating an ad-hoc topology, the accuracy of the analysis on the hypercube largely depends on how well it represents the ad-hoc topology. The following paragraphs describe how a hypercube topology may behave differently than an ad-hoc topology.

First, there are downsides to the compact description of a hypercube. For hypercubes, network properties such as number of nodes and network diameter are a function of the node degree. This rigidity makes approximating ad-hoc networks with disjoint network parameters difficult. For example, assume that there is a network with average node degree, number of nodes, and network diameter of 3, 128, and 25 respectively. A 3-cube, 7-cube, and 25-cube each match one of the ad-hoc network parameters while missing the others. Moreover, there is no hypercube topology that satisfies degree 3, number of nodes 128, and diameter 25. It is reasonable to expect errors in an analytical model using this topology approximation when the ad-hoc topology does not conform to the interrelationship defined by the hypercube topology definition.

Second, it is possible for an ad-hoc network to be partitioned, especially for sparsely deployed networks. By the definition of a hypercube, the topology cannot accommodate partitions and errors are expected to be introduced when using a hypercube topology to approximate a partitioned network. Each partition could become an independent hypercube topology and analyzed separately, but this would require more information for analysis beyond average node degree and number of Black Holes.

Third, a hypercube topology has a uniform node degree, but this cannot occur along the border of the area an ad-hoc network is deployed. From [Bet02], a border effect was noticed when simulating ad-hoc topologies in a 2-D area that violated the author's uniform density assumption. The density of a network is lower along the borders of the operating area because these nodes have a portion of their transmission area is outside of the operating area. Therefore, nodes in this region have a reduced number of neighbors and, as a consequence, the density is lower than the average density in the network. It is expected that the hypercube topology approximation will cause errors in analysis when nodes on the border deviate significantly from the central tendency of the network.

3.4.3 The Hop-Distance Frequency Function for Hypercube Topologies

Let $freq(h,n)$ be a function that computes the number of neighbors that are h- hops from a reference node in an n-cube (a.k.a., hypercube). Function $freq(h,n)$ is piecewise linear and recurrent.

$$freq(h,n) = \begin{cases} 1, & h = 0 \\ freq(h,n-1) + freq(h-1,n-1), & 0 < h \leq n \\ 0, & h > n \end{cases} \tag{10}$$

Since hop count is a positive integer and bounded by the order of the hypercube, every h is mapped to one of three conditions. Function $freq(h,n)$ recursively expands until all branches terminate on conditions $h = 0$ or $h > n$

resulting in either a 1 or 0 respectively. The summation of each leaf is the total number of neighbors in an n-cube that are exactly h-hops from the reference node.

Each condition is described as follows. First, the condition $h = 0$ represents an identity. There is always one node zero hops away from a point of reference in a graph, which is the node itself. The $h > n$ condition is an impossible event by definition of a hypercube because a neighbor's hop-distance cannot exceed the diameter of the topology, which is n [Hwa93].

The remaining condition achieves the bulk of the work by dividing problems into rudimentary computable units. Each recursion of this condition divides the n-cube neighbor frequency problem into two $(n - 1)$-cube sub-problems. Because a hypercube is a binary n-cube, a hypercube can be described as two symmetric $(n - 1)$-cubes. However, the two lower-ordered hypercubes must be joined before they become an n-cube. By adding a *binding link* between each pair of symmetric nodes located in each $(n - 1)$-cube, the structure becomes an n-cube. Figure 3 illustrates this compositional property for a 2-cube, 3-cube, and 4-cube. For each structure, the dashed lines represent the *binding links*.

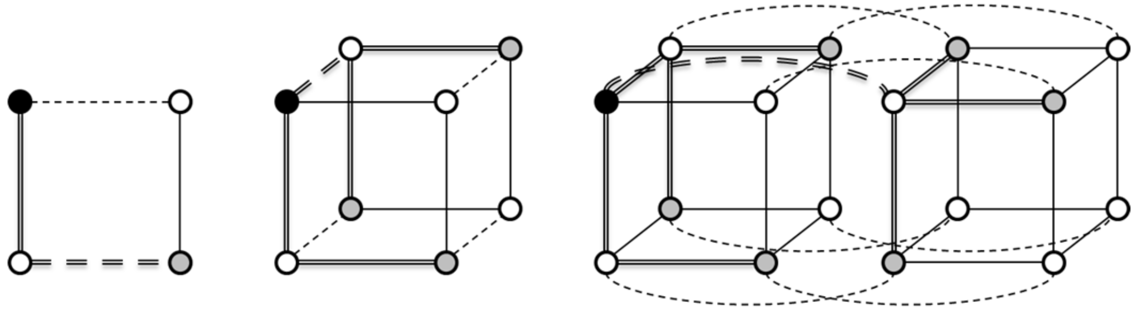

Figure 3: Two-hop neighbors in a 2-cube, 3-cube, and 4-cube topology

Given this compositional property that each n-cube is comprised of two $(n-1)$-cubes, the number of neighbors h-hops away can be generalized as the addition of the number of h-hop neighbors in each lower-ordered hypercube with respect to the *same* reference node. The first sub-problem (i.e., $freq(h, n-1)$) addresses the $(n-1)$-cube containing the reference node. Because of the compositional property, h-hop neighbors in an $(n-1)$-cube are also h-hop neighbors in an n-cube. Therefore, the h-hop neighbors in an n-cube should at least be as many neighbors as h-hop neighbors in an $(n-1)$-cube.

The second sub-problem (i.e., $freq(h-1, n-1)$) addresses the question of how many h-hop neighbors of the reference node are added if the reference node uses its *binding link* to reach the symmetric $(n-1)$ cube. Let the *symmetric reference node* be the adjacent node to the reference node through its *binding link*. Because of the one hop between the reference node and its *symmetric reference node*, the number of h-hop neighbors for the reference node in the symmetric $(n-1)$-cube is the same as the number of $h-1$ neighbors for the *symmetric reference node* in the symmetric $(n-1)$-cube. Adding this sub-problem to the first sub-problem is $freq(h,n) = freq(h, n-1) + freq(h-1, n-1)$, which is the recursion relationship defined in (10).

Figure 3 illustrates the recursive expression for finding all two-hop neighbors in a 3-cube and 4-cube. The black node in each structure denotes the reference node. All gray nodes are the two-hop neighbors of the reference node and each double line indicates a shortest path from the reference node to each two-hop neighbor. Using the recurrence relationship, the number of two-hop neighbors in a 3-cube is the sum of the number of two-hop neighbors in a 2-cube plus the number of one-hop neighbors the adjacent 2-cube. It is easy to see that a 2-cube has only one two-hop neighbor (i.e., $freq(2,2) = 1$). There are two one-hop neighbors in a 2-cube so by (10), $freq(3,2) = freq(2,2) + freq(2,1) = 3$. Likewise, a 4-cube has the same two-hop neighbors as a 3-cube (i.e., $freq(3,2) = 3$) plus all one-hop neighbors in a 3-cube. Since there are three one-hop neighbors in a 3-cube, then there are $freq(4,2) = freq(3,2) + freq(3,1) = 6$ two-hop neighbors for a 4-cube.

Table 1 shows the computation of $freq(h,n)$ for all possible hop-counts for n-cubes where $1 \leq n \leq 10$. Each row represents the neighbor hop-distance frequencies for a particular n-cube and each element in a row is the number of neighbors h-hops from a reference node.

Table 1: Neighbor Hop Distance Frequencies for Hypercubes

n\h	0	1	2	3	4	5	6	7	8	9	10
0	1	0	0	0	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0	0	0	0
2	1	2	1	0	0	0	0	0	0	0	0
3	1	3	3	1	0	0	0	0	0	0	0
4	1	4	6	4	1	0	0	0	0	0	0
5	1	5	10	10	5	1	0	0	0	0	0
6	1	6	15	20	15	6	1	0	0	0	0
7	1	7	21	35	35	21	7	1	0	0	0
8	1	8	28	56	70	56	28	8	1	0	0
9	1	9	36	84	126	126	84	36	9	1	0
10	1	10	45	120	210	252	210	120	45	10	1

There are two things of interest to point out using Table 1. First, it is easy to see the recursive relationship between n-cubes. Any element at row *n* and column *h* is the sum of row $n-1$ column *h* and row $n-1$ column $h-1$. Second, each row is symmetrical, requiring only half that of the elements actually be calculated.

3.4.4 Hop-Distance Density Function for Hypercubes

Given the frequency function for hypercubes, the derivation of the hop distance density function is trivial. It is simply

$$f(h) = \frac{freq(h,n)}{|N|} \tag{11}$$

For example, finding the probability that an arbitrary node in an 5-cube is more than three hops from the reference node is $\frac{3}{16}$. This is because $P[H > 3] = P[H = 4] + P[H = 5]$, $P[H = 4] = \frac{5}{32}$, and $P[H = 5] = \frac{1}{32}$. However, to use the density function to determine the probability that an arbitrary *destination* is h-hops away, the random selection must not include the reference node. In this case, it is an impossible event for a destination to be 0 hops away. Letting the reference node be a source node leaves $|N| - 1$ possible destination nodes. The density function for finding the probability *a randomly selected neighbor* is h-hops away in an n-cube is

$$f(h) = \begin{cases} \frac{freq(h,n)}{|N|-1}, & 0 < h \leq n \\ 0, & h = 0 \end{cases} \tag{12}$$

3.4.5 Comparison of Hop-Distance Density Functions

Because of the previous work in [Bet02], the measured density function of an ad-hoc topology can be compared with a theoretical hypercubes' density function to evaluated compatibility. Figure 4 shows the comparison of density functions for Bettstetter's derivation for a 100 node network, assuming a transmission distance of 250m and an area of 1250m^2. Using the method described in Section 4.2.4, this network has an average degree of 10. Since there are no hypercubes with 100 nodes and degree 10, the hop-distance density function is derived for two hypercubes. One hypercube matches the ad-hoc network's node degree and the other approximately matches the number of nodes as a 7-cube (i.e., 128 nodes).

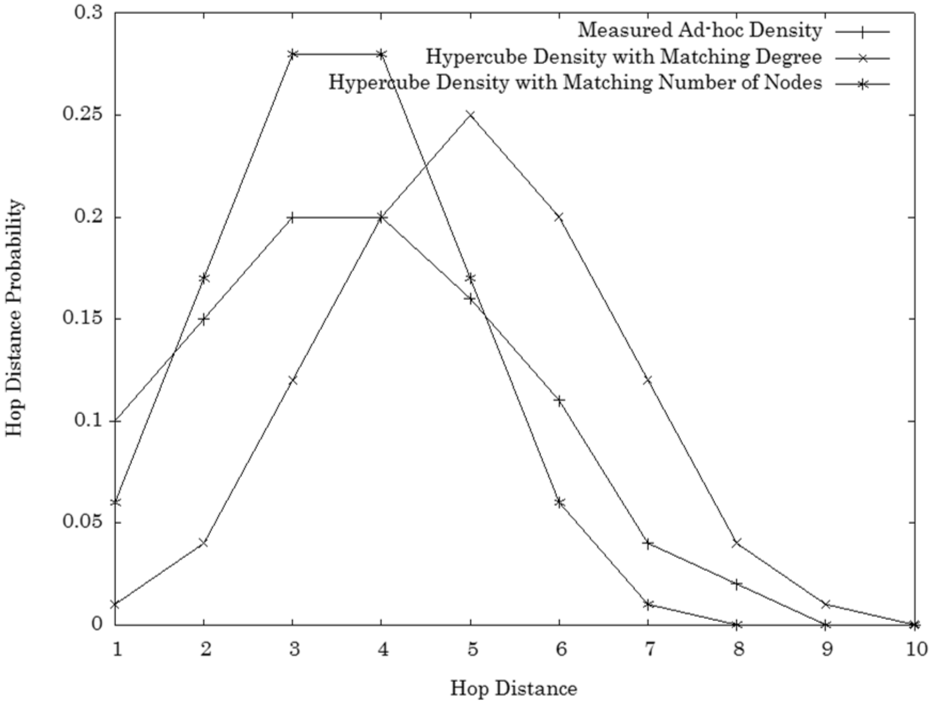

Figure 4: Comparison of Hop-Distance Density Functions

The three lines on the figure show the density functions for 1) the measured ad-hoc topology, 2) a hypercube with the same average node degree as the ad-hoc topology, and 3) a hypercube with the same number of nodes as the ad-hoc topology. In both cases, the hypercube distributions do not match the distribution of the ad-hoc topology, but they may be reasonably close for the purpose of evaluating Black Hole attack effectiveness; however, more significant experimentation is required for conclusive evidence. The figure also suggests that a hypercube with the same number of nodes approximates the mean and a hypercube with matching average node degree approximates the variance of the ad-hoc topology respectively. While this is interesting, it is left as future work to explore, test, and confirm.

3.5 Analytical Black Hole Model for Attractor Phase

Given that a route is being established, an analytical model for the attractor phase of a Black Hole attack determines the probability that the route selected by the protocol is one of the routes submitted by the Black Hole nodes in the network.

Let $P[A]$ be the probability that a route solicited by a Black Hole is selected as the route between an arbitrary source and destination in a network. In other words, let $P[A]$ be the probability that the predicate in (9) is true for an arbitrary source-destination pair. Let H be a random variable describing the distance between a randomly selected source and destination pair, where $1 \leq H \leq n$.

Since

$$P[H=1]+P[H=2]+\cdots+P[H=n]=1$$

Then

$$P[A]=P[A]\{P[H=1]+P[H=2]+\cdots+P[H=n]\}$$

$$P[A]=P[A]P[H=1]+\ P[A]P[H=2]+\cdots+P[A]P[H=n]$$

Applying the conditional probability rule

$$P[A]=P[A|H=1]P[H=1]+P[A|H=2]P[H=2]+\cdots+P[A|H=n]P[H=n]$$

In general

$$P[A]=\sum_{h=1}^{n}P[A|H=h]P[H=h], \tag{13}$$

which is comprised of two parts. First, $P[H=h]$ is the probability that the destination is h-hops away. This has already been derived for hypercube topologies in (12); however, hop-distance density functions for other compatible topologies could also be used to find $P[H=h]$ as they are discovered in future work.

$P[A|H=h]$ is the probability of a Black Hole attack given that the distance between the source and destination is h hops. To find this probability, it can be mapped to a hypergeometric distribution. For a hypergeometric distribution, there are a number of items in a *pool*, where a known quantity of items have a *desired trait* and the remaining proportion of the population does not. A hypergeometric experiment consists of sampling a subset of the items from the total *pool* of items. A hypergeometric random variable is the number of *sampled items* that have the *desired trait*.

Let the hypergeometric experiment be a route discovery attempt by a source to a destination node that is h-hops from the source. Let the *pool* be the number of nodes in the network excluding the source and destination node. From Theorem 2, let the *desired trait* be all nodes closer to the source than the destination is to the source. Let r be the number of nodes having the *desired trait* in the network. Since the destination is h-hops from the source, this is simply

$$r = \begin{cases} \sum_{i=1}^{h-1} freq(i,n), & h > 1 \\ 0, & h = 1 \end{cases} \tag{14}$$

Let the number of *sampled items* in the hypergeometric experiment be the number of Black Hole nodes in the network. Finally, Let K be a hypergeometric random variable of the number of Black Hole nodes having the *desired trait*. In general, the probability that exactly k Black Hole nodes are closer than the destination is

$$P[K = k|\, H = h] = \frac{\binom{r}{k}\binom{(|N|-2)-r}{|B|-k}}{\binom{|N|-2}{|B|}} \tag{15}$$

From [MiA03], this hypergeometric distribution is subject to the constraint

$$\max[0, |B| - ((|N| - 2) - r)] \leq k \leq \min(|B|, r) \tag{16}$$

From Theorem 2, a Black Hole attack will occur if at least one Black Hole has the *desired trait*. Therefore

$$P[A|H = h] = P[K \geq 1|H = h] \tag{17}$$

As a hypergeometric problem, $P[A|H = h]$ is equivalent to

$$P[K \geq 1|H = h] = 1 - P[K = 0|H = h] = 1 - \frac{\binom{r}{0}\binom{(|N|-2)-r}{|B|}}{\binom{|N|-2}{|B|}} \tag{18}$$

Substituting (18) and (12) into (13) reveals the analytical Black Hole attack model for hypercube topologies:

$$P[A] = \sum_{h=1}^{n} \left\{ \left[1 - \frac{\binom{(|N|-2)-r}{|B|}}{\binom{|N|-2}{|B|}} \right] \frac{freq(h,n)}{|N|-1} \right\} \tag{19}$$

Because $k = 0$ in (18), both (18) and (19) are valid only when

$$\max[0, |B| - ((|N| - 2) - r)] \leq 0 \leq \min(|B|, r) \tag{20}$$

3.5.1 Attractor Model Example Computation

This model can find the probability a route discovery process is corrupted by a Black Hole given the dimensionality of the hypercube and the number of Black Holes. For example, let there be three Black Hole nodes in a 4-cube. In this case, h can exist from one to four, the cardinality of N is 16, and the cardinality of B is 3. For the case where $h = 1$, Equation (14) indicates that $r = 0$ because no neighbors can be closer than one hop from the source node and from Table 1 $freq(1{,}4) = 4$. Therefore for $h = 1$

$$P[A|H = 1] = \left[1 - \frac{\binom{(|N|-2)-r}{|B|}}{\binom{|N|-2}{|B|}} \right] \frac{freq(h,n)}{|N|-1} = \left[1 - \frac{\binom{14}{3}}{\binom{14}{3}} \right] \frac{4}{15} = 0$$

For $h = 2$

$$P[A|H=2]=\left[1-\frac{\binom{10}{3}}{\binom{14}{3}}\right]\frac{6}{15}=0.268$$

For $h=3$

$$P[A|H=3]=\left[1-\frac{\binom{4}{3}}{\binom{14}{3}}\right]\frac{4}{15}=0.264$$

For $h=4$

$$\max\left[0,|B|-\left((|N|-2)-r\right)\right]=3$$

and

$$\min(|B|,r)=3$$

For $h=4$ the predicate in (20) is false because $3 \leq 0 \leq 3$ is not true. This means that the hypergeometric distribution cannot be used. Fortunately, calculating $P[A|H=4]$ for this condition is trivial. Table 1 indicates that when $h=n$ *all* remaining nodes (i.e., $|N|-2$) are between the source and destination. Therefore $P[A|H=4]=1$ and in general $P[A|H=n]=1$. With this knowledge, for $h=4$

$$P[A|H=4]=1*\frac{1}{15}=0.066$$

The resulting summation for all h is $P[A]=0.598$. This means that approximately 60% of routes in the hypercube network will fall victim to a Black Hole attack.

3.5.2 Analytical Results of Attractor Model

Figure 5 shows the analytical results using the Attractor Model for hypercubes of orders ranging from 5 to 30 and $0 \leq |B| \leq 15$. For clarity, only hypercubes of orders divisible by five are depicted. The x-axis of the figure indicates the number of Black Hole nodes in the hypercube. The y-axis is $P[A]$ and each line shows $P[A]$ for a given hypercube and number of Black Hole nodes.

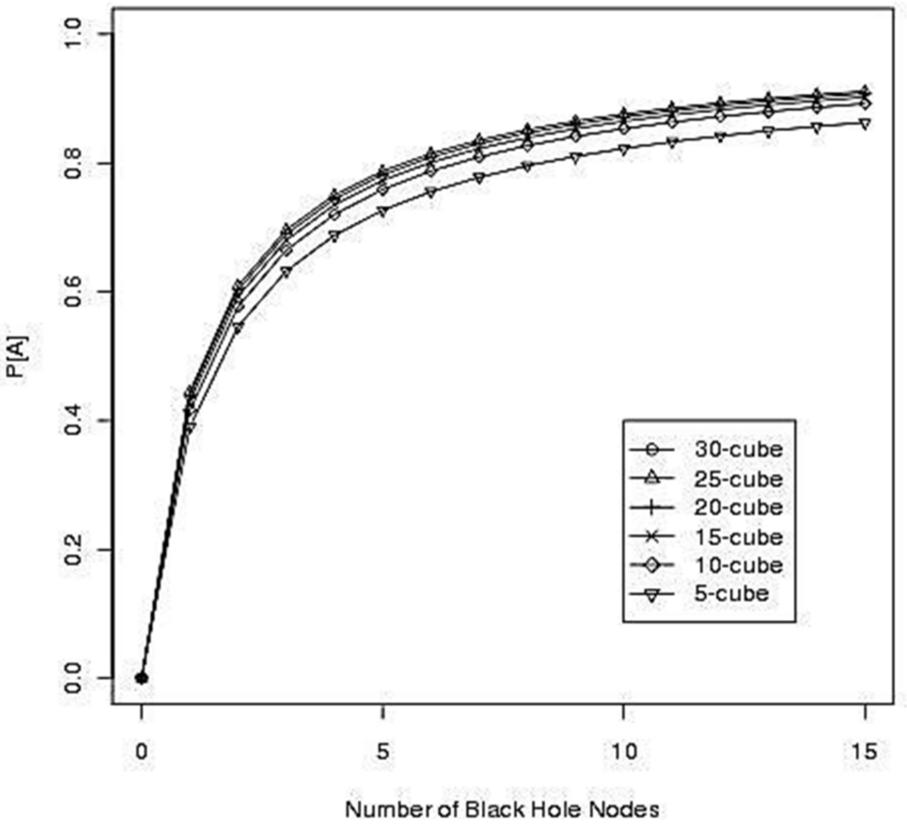

Figure 5: Attractor Model Results

The results in Figure 5 reveal several things. First, as either the order of the hypercube or the number of Black Hole nodes increase, $P[A]$ increases. While it is intuitive that increasing the number of Black Holes increases performance, the relationship between the order of the hypercube and $P[A]$ is more elusive. The model indicates that Black Hole nodes benefit more from higher degree, more nodes, and an increasing diameter more than the destination. A larger n provides slightly more opportunities to be closer to the source than the destination.

A second observation is that as the number of Black Holes and the order of the hypercube increases, the relative performance gain of $P[A]$ decreases. As these parameters increase, $P[A]$ converges on a maximal value. The significance of this is that a theoretical upper-bound may be identified given one parameter is fixed and the other is a free variable. For example given five Black Holes, the best $P[A]$ regardless of the hypercube order converges upon 79%. Alternatively the upper-bound probability of Black Hole attack given a hypercube of order 30 converges on 95%.

3.6 A Simple Model for the Exploitation Phase in Hypercube Networks

Given that one knew with certainty which routes are under Black Hole attack, then the performance degradation is simply the proportion of traffic transmitted over the corrupted routes versus all forwarded packets in the network. However, the analytical model presented in Section 3.5 only determines the probability a randomly selected route in a network is subject to Black Hole attack and does not identify which particular routes are corruptible. Therefore, this simple model applies the Attractor Phase model to determine packet loss at the network level.

Let R be a random variable for the number of routes in the lifetime of a network. Let C be a binomial random variable representing the number of successful routes commandeered by a Black Hole attack. The density function for C is

$$f(c) = \binom{E[R]}{c} P[A]^c (1 - P[A])^{E[R]-c} \tag{21}$$

For C to be binomial, it is assumed that the number of routes in a network is fixed, routes that are formed do not affect $P[A]$ for subsequently formed routes, and all non-malicious nodes have equal probability of becoming a source or destination in a given route.

Since C is binomial, the expected number of routes taken over is

$$E[C] = P[A]E[R] \tag{22}$$

Let S and D be random variables for the number of packets transmitted by the source and the number of packets dropped by Black Hole attack respectively in an arbitrary route. The relationship between these random variables is

$$E[D] = P[A]E[S] \tag{23}$$

Let D_N be a random variable for the total number of packets dropped by a Black Hole attack for all routes. The overall network effect of a Black Hole attack is simply

$$E[D_N] = E[C]E[S] \tag{24}$$

For example, using the example calculation from Section 3.5.1, let $P[A] = 0.598$. Let $E[R] = 8$ and $E[S] = 4000$. Table 2 shows the densities for C. From this distribution, questions can be answered about the probability that a certain number of routes in the network will be subject to Black Hole attack. For example, the probability that at least one route is subject to Black Hole attack is

$$P[C \geq 1] = 1 - P[0] = 0.999$$

Table 2: Density of $C, 0 \leq c \leq 8$

c	$P[C = c] = f(c)$
0	$6.82x10^{-4}$
1	$8.12x10^{-3}$
2	$4.23x10^{-2}$
3	$1.26x10^{1}$
4	$2.34x10^{1}$
5	$2.78x10^{1}$
6	$2.07x10^{1}$
7	$8.79x10^{-2}$
8	$1.63x10^{-2}$

The expected number of routes under attack for this network is

$$E[C] = P[A]E[R] = 4.78\, routes$$

The expected number of packets dropped by Black Hole attack for an arbitrary route is

$$E[D] = P[A]E[S] = 2392\, packets$$

The expected overall effect a Black Hole attack for the network is

$$E[D_N] = E[C]E[S] = 19120\, dropped\, packets$$

IV. Methodology

An experiment is conducted to test the hypothesis that the analytical Black Hole Attractor Model derived in Chapter III can determine performance loss of ad-hoc networks. Simulation is the most appropriate method for experimentation because it would otherwise be very expensive to setup, validate, and test enough real ad-hoc topologies to make statistical inferences about the hypothesis.

The remainder of this chapter is organized as follows. Section 4.1 describes the system under test for the experiment. This includes which component is being tested, the implementation of the Black Hole simulation models, and a small experiment to validate the implementations. Section 4.2 describes the experiment design, methodology, and a brief narrative describing the process.

4.1 System Under Test

The system under test for this experiment is a wireless ad-hoc network that is simulated using Network Simulator 2.34 [Net11]. The network contains a known number of nodes deployed randomly in an area using the *setdest* program, which is included in the simulation package. *Setdest* places nodes in an area by sampling the Cartesian coordinates from uniformly random variables. Once placed, each node remains in its position for the duration of the simulation.

Each wireless ad-hoc node in the network is a simulation model, which is comprised of an antenna, radio, propagation model, and a protocol stack to communicate with each other in Network Simulation 2.34 (a.k.a., ns-2). Specifically, the stack is comprised of an omni-directional antenna with unity gain, a 914MHz Lucent WaveLAN DSSS radio, an implementation of IEEE 802.11 Medium Access Control (MAC) layer, and a reactive MANET routing protocol. The stack enables each node to provide packet routing for the wireless ad-hoc network. Besides basic routing services, some nodes are designated as *application end-points*, which send or receive constant bit-rate (CBR) traffic. A *Black Hole* is a node with a modified MANET routing protocol designed to conduct Black Hole attacks and is never an application end-point.

4.1.1 Component Under Test

The component under test for this experiment is a route in an ad-hoc network. The treatment on the route is the relative locations of the source, destination, and Black Hole nodes that participate in the route discovery process. Since the ad-hoc topologies are randomly generated, treatment is random for all routes under test.

For each randomly generated topology, every possible source and destination pair is tested to see if it is subject to Black Hole attack. This exhaustive method is preferred over random sampling because 1) the population of possible routes is small because of the low number of nodes, and 2) random sampling of source-destination pairs introduces an additional level of randomness. The additional randomness confounds the effects of the intentionally random treatment, so it is avoided. The frequency of Black Hole attacks collected during treatment for every source-destination pair over multiple ad-hoc topologies is compared with the predictions of the analytical attractor model to evaluate its accuracy.

One confounding source of randomness in the component under test is the random delay incurred at each hop of a RREQ broadcast. The random delay minimizes the risk of collisions between two neighbors that hear the same RREQ and rebroadcast it at the same time. Broadcast collisions are not detected by IEEE 802.11, so this random delay must exist to avoid nodes disrupting their neighbors' rebroadcast of the RREQ. The consequence of this randomness is that a node may receive a RREQ after another node with a larger hop-distance to the source node. While this does not affect Lemma 3, the behavior does not fit the assumptions in Lemma 4 and consequently Theorem 2. As a result, there is some probability that Theorem 2 does not hold for an arbitrary route in a network that uses a reactive MANET protocol. This experiment accounts for the unwanted randomness by treating it as sampling bias, which is alleviated by selecting the appropriate number of experiment replications. The process for this is covered in Section 4.2.3; however, quantifying the probability of that a node receives a RREQ after a node with a greater hop-count to the source should be studied in future work and applied to this model.

4.1.2 Black Hole Node Implementation

Two Black Hole Attack simulation models are implemented for ns-2 by extending the AODV and DSR protocol simulation models included in the ns-2 distribution.

4.1.2.1 DSR Black Hole

A DSR Black Hole listens on its radio interface for arriving packets. When a packet arrives, it handles it in one of several ways, depending on the packet type. If the packet is a RREQ packet, it immediately generates a false source route to the requestor. This is accomplished by generating a RREP packet with the destination of the RREQ set as the source of the RREP. Before copying the source route in the RREQ packet, the Black Hole node appends itself and the destination to the route. It places the reverse of the resulting route in the spoofed RREP packet and then places it in its send queue. This behavior implements the *Attractor Phase* discussed in Section 2.2.

If the arriving packet is not a DSR protocol coordination packet, but rather an application packet to be forwarded, it silently drops the packet. This behavior implements the *Exploitation Phase* discussed in Section 2.2.

The Black Hole node is a protocol compliant DSR implementation for all other packets. To accomplish this, the node's cache must not be tainted with false routing information. Therefore, the Black Hole node only stores the correct portion of the reverse source route in its cache (i.e., the segment between the source and Black Hole node). Second, the Black Hole node avoids cache snooping (i.e., placing overheard source routes in its cache) because the Black Hole cannot be certain that an overheard route is a valid route or one generated by another Black Hole node in the network.

4.1.2.2 AODV Black Hole

An AODV Black Hole listens on its radio interface for arriving packets. When a packet arrives, it handles it in several ways, depending on the packet type. If the packet is a RREQ, the Black Hole immediately begins generating a false RREP. One significant issue for the Black Hole is to guess the destination's actual sequence number. Methods for doing this are discussed in Section 3.2.3 and in [KHK09]; however, this implementation of an AODV Black Hole relies on the fact that the destination sequence numbers for all nodes in ns-2 running AODV begin at 2. If the simulation scenario is constructed to only have a single connection attempt for the entire experiment, then the Black Hole knows that the destination's sequence number must be 2. This behavior is equivalent to a Black Hole that is able to perfectly predict sequence numbers of any destination, making route selection in AODV purely about hop-count. When it receives the RREQ, the AODV Black Hole places this initial destination sequence number into the RREP. The Black Hole initializes the hop count to 2 in the RREP so that it will make the destination appear one hop from the Black Hole node to all nodes along the reverse path to the source node. Before placing the RREP on the send queue, the source and destination of the RREP are set to the destination and source of the RREQ respectively.

If the packet is not an AODV coordination packet, the Black Hole node silently drops the packet. Like the DSR Black Hole, the AODV Black Hole is protocol compliant for all other packet types. The Black Hole node accomplishes this by not corrupting its own routing table. For example, when issuing the RREP, it does not add this distance vector entry to its table. When replying to a RREP spoofing the destination, it does not update its own destination sequence number.

4.1.3 Simulation Validation

To validate the setup of the system under test in ns-2, a portion of the experiment in [CPZ09] is conducted using the implemented Black Hole simulation models. Cai's experiment involved simulating a Black Hole attack for a DSR MANET of 50 nodes in a 1000m^2 area. The number of Black Holes in the network was a factor with selected levels as powers of 5. One of the response variables Cai measured was packet loss percentage, which is simply the ratio of packets dropped due to Black Hole attack versus the number of packets sent by all source nodes.

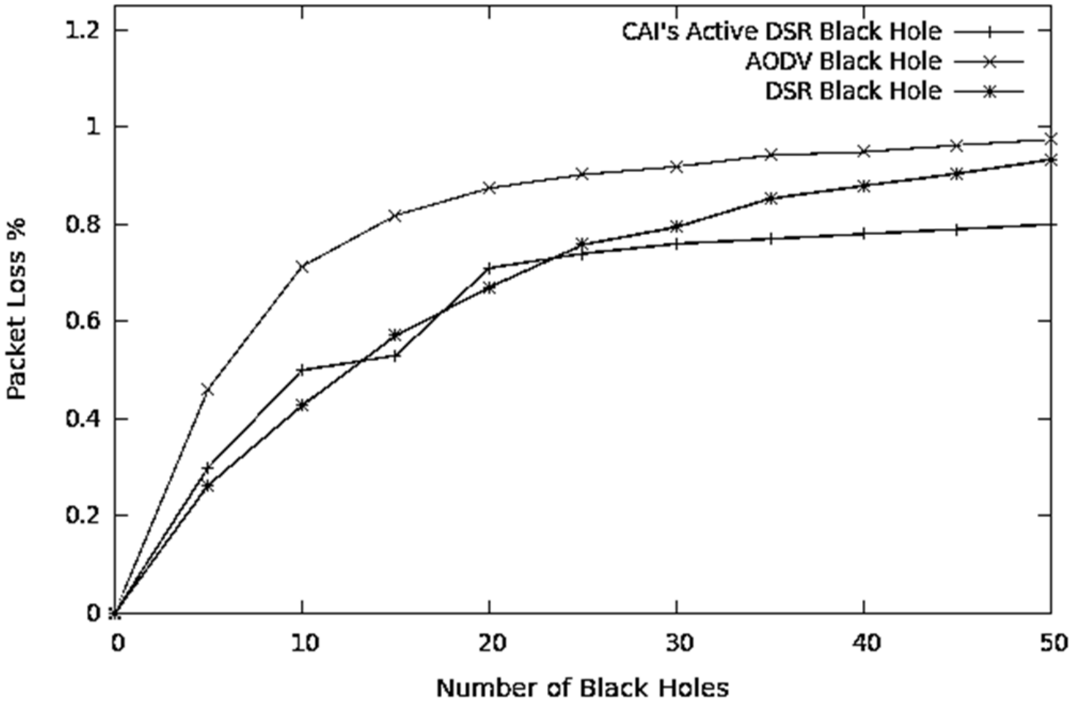

Figure 6: System Under Test Validation using Cai's Experiment

The validation is conducted via simulation for each Black Hole simulation model and for all Black Hole levels. Each factor level combination is replicated 100 times to derive the average packet loss percent for the given levels. The results are shown in comparison to Cai's original results in Figure 6. The data shows both the AODV and DSR Black Hole models exhibit similar growth in packet loss as the number of Black Hole nodes is increased. However, there is a noticeable difference between the performance of the AODV and DSR Black Hole attacks. This will be problematic for the analytical Black Hole model because it does not account for these differences.

4.2 Design of Experiment

The experiment is a full factorial experiment that measures *Packet Loss Percentage, a statistical measurement of* $P[A]$ and *Received Packet Percentage*. The selected factors are average node degree, MANET protocol, and number of Black Holes; the selected factor levels are shown in Table 3.

Table 3: Selected Factor Levels

Average Node Degree	{4,6,8,10}
MANET Protocol	{AODV, DSR}
Number of Black Holes	{0,1,2,5,10}

To compute $P[A]$, the attractor model requires the number of Black Holes in the network and the average node degree. Since these are parameters of the analytical model, they are included as factors for the experiment to test different values of $P[A]$. The levels for these factors are selected based on the tradeoff between validating every data point in Figure 5 and the computational limitations of the machine hosting the simulation. The protocol is selected as a factor to determine if the model applies to more than one reactive MANET protocol and the levels cover both AODV and DSR, which are prototypical instantiations of the reactive MANET protocol class.

4.2.1 Experiment and Simulation Parameters

Table 4 lists the parameters used for the experiment and for each simulation within the experiment. Because this is a full factorial experiment, the number of factor level combinations is 40, which is the product of the number of levels for each factor. The number of replications is determined experimentally in Section 4.2.3. The number of simulations per replication is based on the need to simulate each possible source-destination pair in a given network topology. Using the nomenclature from Section 3.5, the number of simulations per replication is

$$|E| * |E| - 1 \tag{25}$$

where E is the set of non-malicious nodes in the network. In this case, depending on the factor level for number of Black Holes, there are 40, 39, 38, 35, and 30 benign nodes respectively. This results in $(40 * 39), (39 * 38), (38 * 37), (35 * 34)$, and

(30 ∗ 29) possible source-destination pairs for scenarios with 0, 1, 2, 5, and 10 Black Hole nodes respectively.

Table 4: Selected Experiment and Simulation Parameters

Factor Level Combinations	40
Replications per Factor Level Combination	50
Simulations per Replication	1560, 1482, 1406, 1190, 870
Number of Nodes	40
Simulation Duration	500 seconds
Traffic Sources	1 per simulation
Traffic Type	Constant Bit Rate
Traffic Rate	2.44 packets per second
Packet Size	512 Bytes
Data Rate	10 Kbps
Traffic Start Time	0
Traffic End Time	450 seconds
Mobility	None

The values for simulation duration, node size, and traffic rate are selected based on values selected in prior published work in [CPZ09], [BhS09], and [DSE07]. They are considered reasonable parameters for a modern ad-hoc network. The CBR traffic source ceases sending packets at 450 seconds into a simulation to permit time for the packets in the system to be flushed out of the network. This value is selected via observations of trace files from earlier pilot studies.

4.2.2 Response Variables

Because the purpose of the experiment is to test the analytical model, the predictions of the model must be tied to measurable output variables in the simulation. The two response variables *Packet Loss Percentage* and *Received Packet Percentage* measure the performance of an arbitrary route in a network. From (23), $P[A]$ can be isolated to be of the form

$$P[A] = \frac{E[D]}{E[S]} \tag{26}$$

Since every possible connection is simulated for a given topology, the population means of the number of dropped packets and number of sent packets can be computed. Let $\mu_{D,i}$ and $\mu_{S,i}$ be the population means of the topology generated in replication i for the average number of packets dropped and sent respectively. Let *Packet Loss Percentage* be a statistical measurement of $P[A]$ and a response variable of the experiment. From (26), the point estimator for $P[A]$ is

$$\widehat{P[A]} = \frac{\mu_{D,i}}{\mu_{S,i}} \tag{26}$$

Given r replications, *Packet Loss Percentage is*

$$Packet\ Loss\ Percentage = \frac{\sum_{i=1}^{r} \frac{\mu_{D,i}}{\mu_{S,i}}}{r} \tag{27}$$

A second response variable is *Received Packet Percentage*, which is the proportion of packets received by destination nodes in a route over the number of packets sent in the route. Let $\mu_{R,i}$ be the population mean of a given topology in replication i for the average number of received packets in a route. Given r replications, *Received Packet Percentage* is measured as

$$Received\ Packet\ Percentage = \frac{\sum_{i=1}^{r} \frac{\mu_{R,i}}{\mu_{S,i}}}{r} \tag{28}$$

This response variable is used to support *Packet Loss Percentage* by ensuring that the intended effect of a Black Hole attack (i.e., lost packets) is actually occurring. If the Black Hole attack is truly dropping packets, then it is expected that the number of packets received is negatively correlated with the number of packets dropped by Black Hole attack.

Upon completion of a simulation, ns-2 generates a packet trace file containing all events that occurred for each packet in the simulation. Events such as a new packet being sent on the network, the destination receiving the packet, and a Black Hole dropping the packet are all captured in the trace file and can be counted for each simulation.

During each replication, $\mu_{D,i}$, $\mu_{S,i}$, and $\mu_{R,i}$ are calculated after the simulation results for all possible source and destination pairs that have been collected.

4.2.3 Method for Determining Number of Replications

To account for random variation, the experiment is repeated several times using different random seeds to estimate the mean of each response variable. However, if the experiment is not repeated enough times, significant sampling bias will be inserted into the data, making it difficult to justify conclusions on the collected data. A common approach to determine a reasonable number of replications is to:

1. Estimate a good number of replications.
2. Run an experiment so that multiple groups of replications can be generated.
3. Find the confidence intervals of response variables for each replication group.
4. Compare all groups with each other to identify sampling bias.

Sampling bias is minimized if the confidence intervals generally overlap and the interval distances are similar between independent experiments. If they are not, then the number of replications is increased and the process is repeated until the desired stability is achieved.

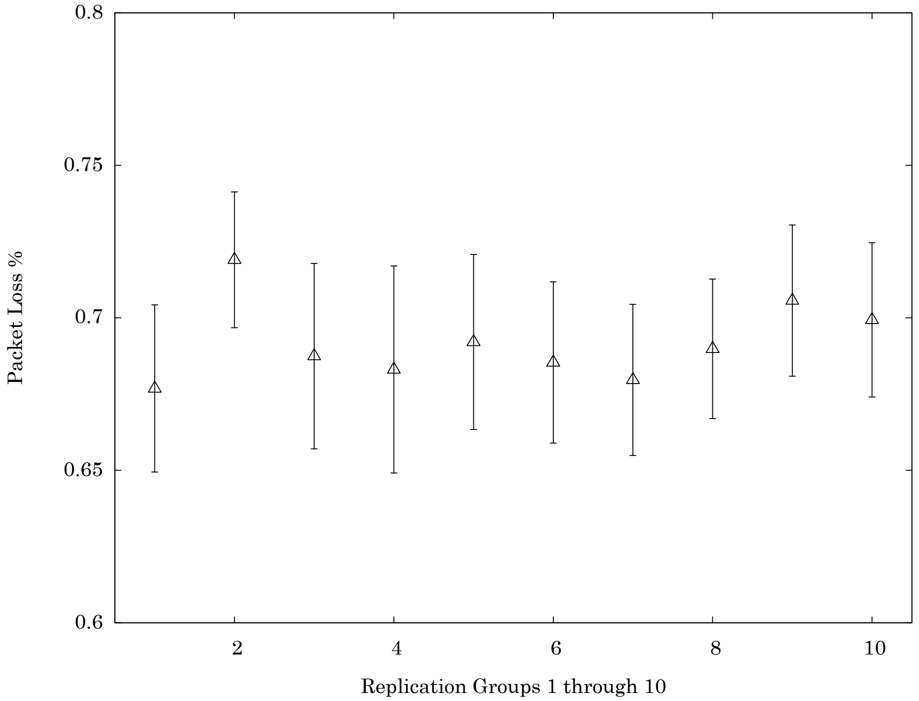

Figure 7: Packet Loss Percentage for 10 groups with 50 replications

Using the process described above, this experiment requires 50 replications to minimize sampling bias. Figure 7 shows the 95% confidence intervals for the mean *Packet Loss Percentage* for each of the 10 groups of 50 replications. Each replication of an experiment involved generating a random ad-hoc topology containing 40 nodes in a 750 m^2 area with one Black Hole and independently simulating all possible connection pairs. The figure shows that the confidence intervals overlap and are of similar length, implying that sampling bias is minimized.

4.2.4 Method for Determining Average Node Degree

Methods such as the uniform density assumption in [Bet02] can be used to find the expected node degree of an ad-hoc topology; however, the model erroneously overestimates the node degree because it does not account for the border effects. To avoid introducing this error into the experiment, average node degree is instead determined experimentally through simulation.

Node degree is a function of the area and number of nodes deployed in the area. Consequently, there are multiple solutions for a given node degree. To find solutions, the number of nodes is fixed at 40 and multiple small experiments are conducted to find areas that result in the average degree matching each of the desired levels. Each experiment consists of generating several random topologies using the *setdest* program given the number of nodes and operating area. For each random topology, the output topology file from *setdest* is analyzed to derive a sample of the *average node degree* of the given parameters. Several samples are collected to determine the average node degree of a random topology. The error between the calculated and expected degree is used to refine the search for the correct area value. After several iterations of experimentation, the process converges on areas that result in the desired *average node degree*. The process identifies that for a network of 40 nodes, areas of 1267m^2, 1005m^2, 850m^2, and 750m^2 provide an average node degree of 4, 6, 8, and 10 respectively.

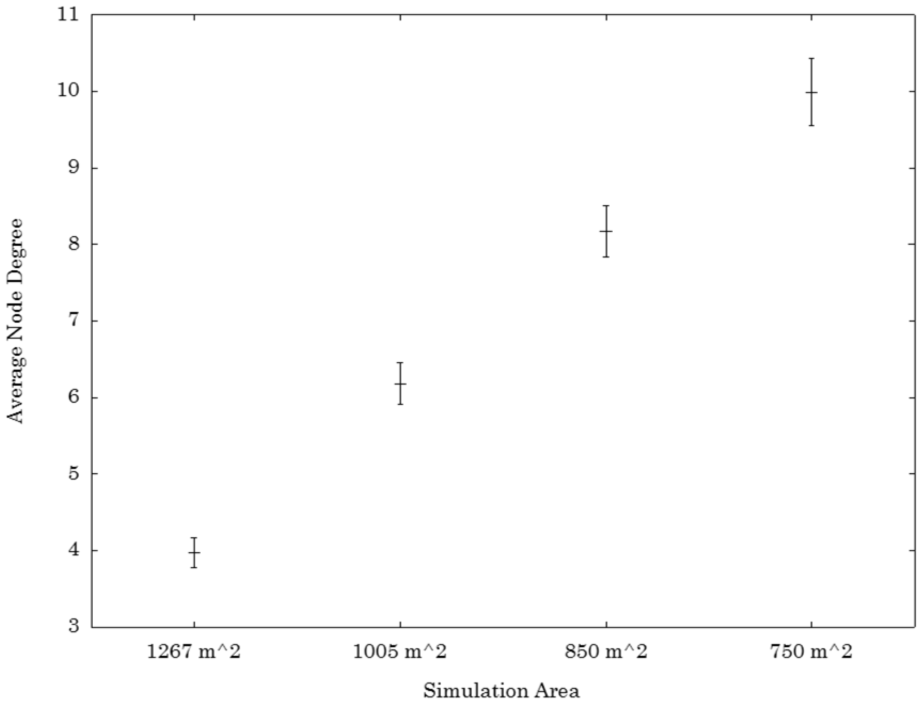

Figure 8: Areas for 40 Node Network to Achieve Node Degree

Figure 8 shows the 95% confidence intervals for the mean *average node degree* given the selected area size. The intervals are taken from sampling randomly generated topologies containing 40 nodes and finding the average node degree. The figure shows that even for a small sample size of 50, the confidence interval for the mean *average node degree* contains the desired *average node degree* without significant error.

4.2.5 Experiment Process

For each factor level combination, a series of replicated experiments are performed to minimize sample variation and result in an statistical measurement of $P[A]$: *Packet Loss Percentage*. Each replication generates a new random ad-hoc network topology based on the selected factor levels. Thus, the difference between replications of the same factor level combination are the relative distances of the source, destination, and Black Hole nodes.

For each replicated experiment, every possible source-destination pair in the network is simulated individually using the same topology and the number of packets sent by the source, received by the destination, and dropped by the a Black Hole node are recorded. Rather than simulate a single scenario where all possible connection pairs attempt to connect to each other, each individual connection pair is evaluated independently in its own simulation instance. This setup avoids confounding effects such as congestion between each connection pair or excessive congestion around the Black Hole nodes.

Each unique single pair scenario involves the source sending constant bit rate traffic to the destination. Depending on the relative locations of the source, destination, and the Black Hole nodes, packets may be dropped due to Black Hole attack. After the scenario is simulated, the resulting trace file is examined to collect the number of sent, dropped, and received packets for that route. After the results for all possible connection pairs are simulated, μ_R, μ_S, and μ_D are calculated for the replication to generate a sample for *Packet Loss Percentage* and *Received Packet Percentage*. The samples for *Packet Loss Percentage* and *Received Packet Percentage* are averaged to provide an estimation of *Packet Loss Percentage* and *Received Packet* for the given factor level combination.

V. Results and Analysis

The experiment is executed and the metrics are collected using the setup and process described in Chapter IV. The contents of this chapter are as follows: Section 5.1 presents the results, provides immediate observations about the data, and analyzes the error between the model and experiment to identify areas for further study. Section 5.2 utilizes the experimental results to briefly evaluate an alternate form of the hypothesis. Section 5.3 summarizes the inferences made from the data. Section 5.4 applies the inferences to evaluate the hypothesis.

5.1 Experiment Results and Observations

Figures 9 through 12 show the results obtained by the experiment. The x-axis in each figure is the number of Black Holes and the y-axis is a percent value that captures both metrics *Packet Loss Percentage* and *Received Packet Percentage*. In each figure the 95% confidence intervals of the estimation of the mean *Packet Loss Percentage* for both AODV and DSR protocols are plotted against the results derived from the analytical hypercube model. Additionally, the sample mean of *Received Packet Percentage* is plotted on the same graph to show the effect of the Black Hole attack.

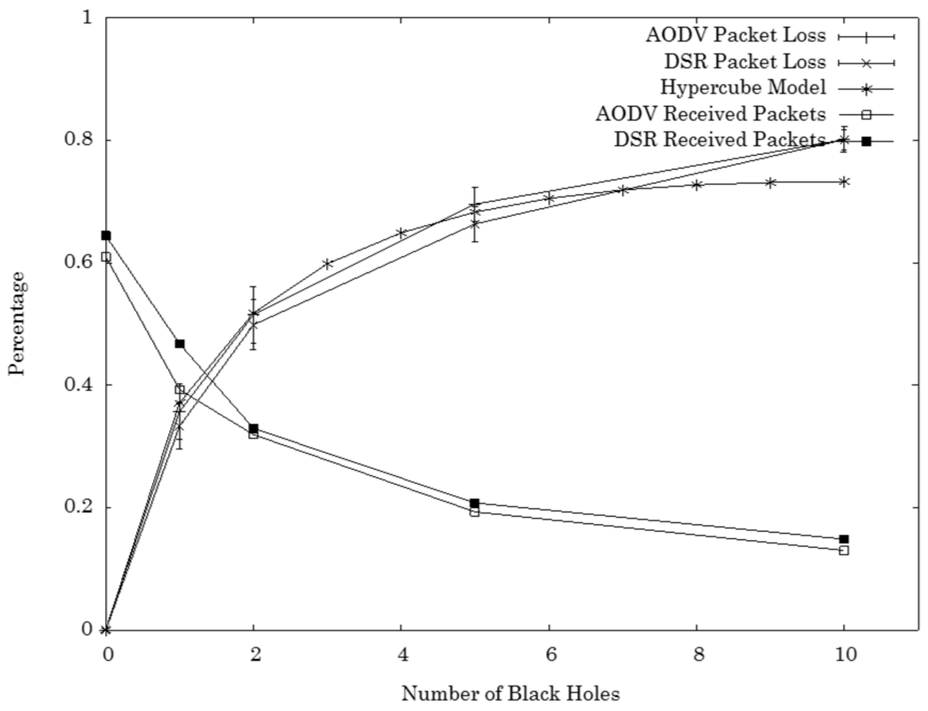

Figure 9: 4-Cube Model versus Ad-hoc Network with Average Degree 4

Figure 9 depicts the results obtained for all MANET protocol levels, all Black Hole levels, and Average Node Degree 4 using an area of 1267m^2. The figure shows that *Received Packet Percentage* decreases as the number of Black Hole nodes increase for both protocols. Even without Black Holes, only 60% of the traffic arrives at its destination. Since the network has low density, it is possible that there are no routes between a source-destination pair due to network partitioning. Experiments involving higher node degree (i.e., smaller area) result in higher density and lower probability of network partitioning. The minimization of this probability allows *Received Packet Percentage* to approach 1.0 as the average node degree increases.

When the factor Average Node Degree is 4, the 4-cube model falls within or very close to the 95% confidence interval of the measured *Packet Loss Percentage* where the number of Black Holes is 1, 2, and 5. However, the analytical model does not predict the correct performance results when there are 10 Black Holes.

Figure 10 shows the performance results when the factor Average Node Degree is 6 for all protocol and Black Hole levels. As expected, *Received Packet Percentage* decreases as the number of Black Holes increase. The metric also shows that topologies of this class are less likely to be partitioned than 40-node topologies using an area of 1267m^2. While the 6-cube analytical model falls within the confidence intervals for AODV *Packet Loss Percentage*, the model does not correctly describe Black Hole performance for the DSR protocol.

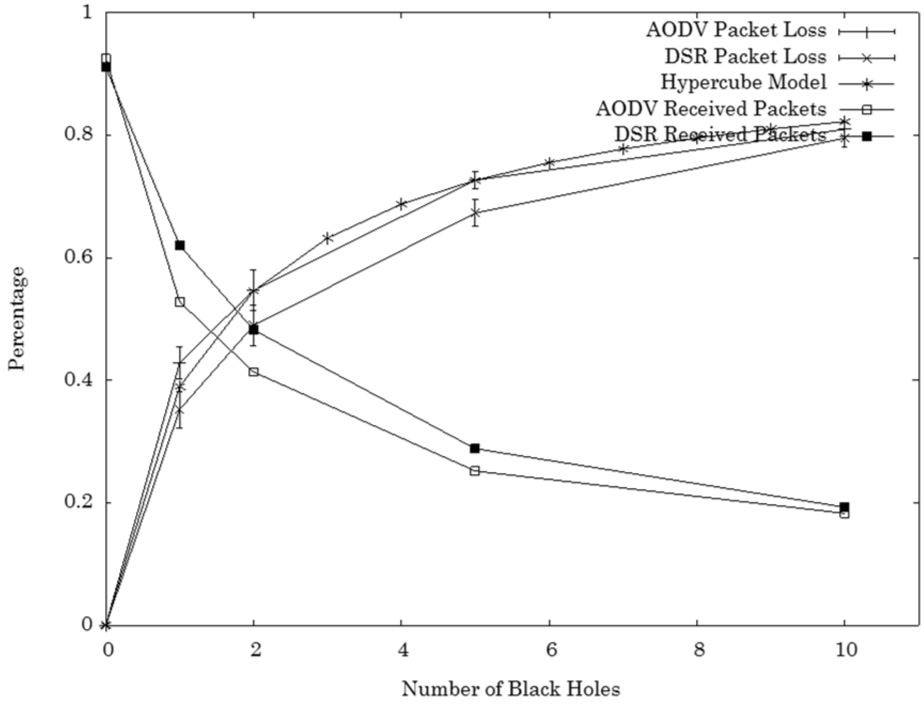

Figure 10: 6-Cube Model versus Ad-hoc Network with Average Degree 6

Figure 11 and Figure 12 exacerbate the issues exposed in Figure 10. The 8-cube and 10-cube analytical models do not accurately describe the behavior of *Packet Loss Percentage* for either protocol when the average node degree is 8 and 10 respectively.

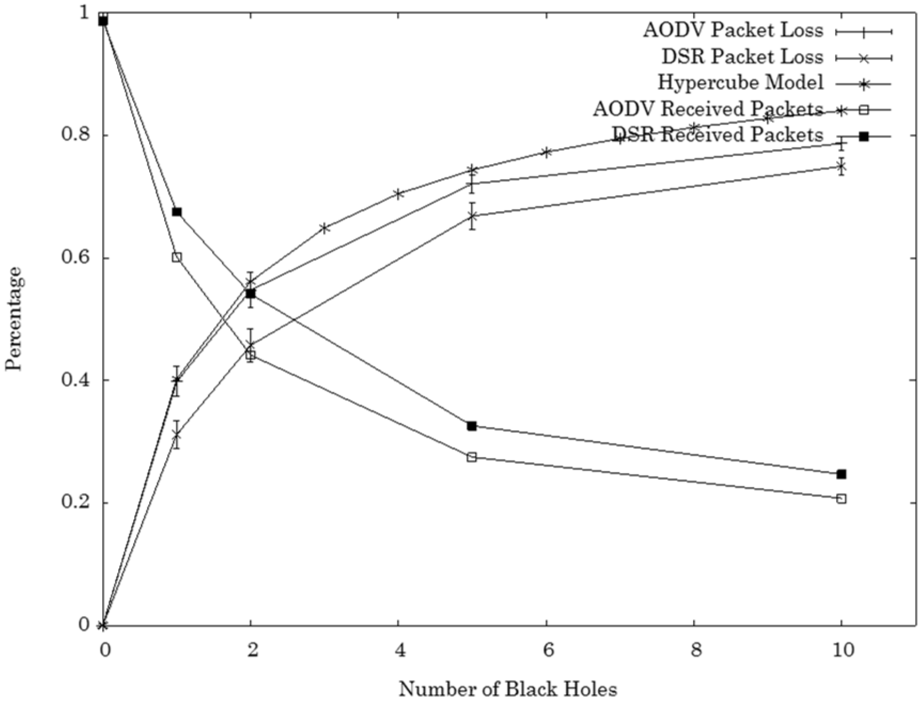

Figure 11: 8-Cube Model versus Ad-hoc Network with Average Degree 8

5.1.1 Observations on Results

Overall, the model matches the order of growth for all experimental results. As the number of Black Hole nodes increase, the expected packet loss increases logarithmically. While the 4-cube and 6-cube model fits well with the experimental results, the 8-cube and 10-cube do not. In fact, the difference between the model's predication and the experiment results increases as the degree increases.

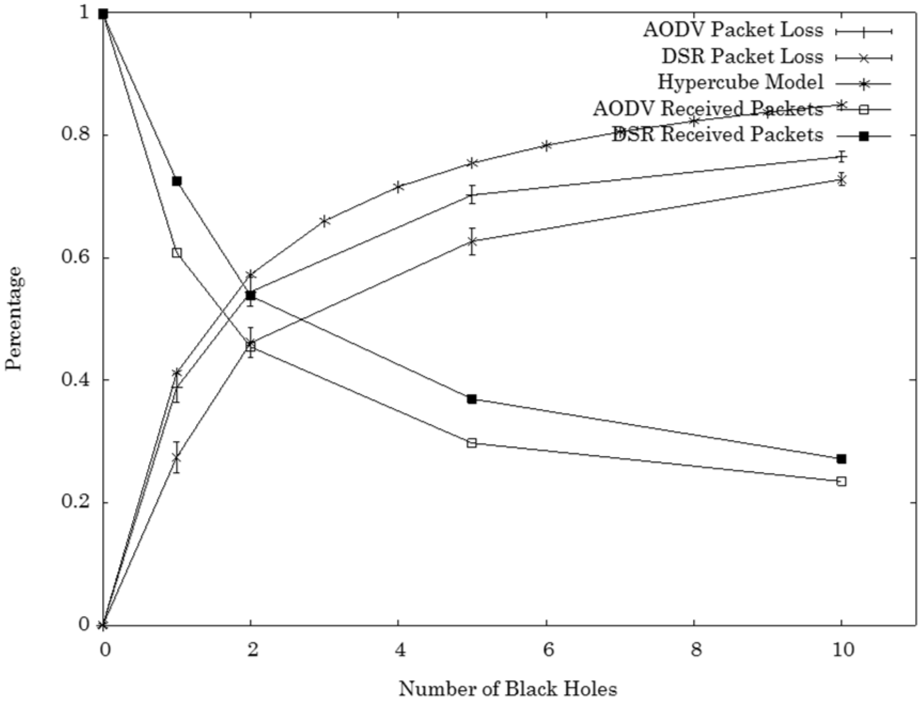

Figure 12: 10-Cube Model versus Ad-hoc Network with Average Degree 10

5.1.2 Inferences on the Experiment Results

Because the model can predict the order of growth in performance as the number of Black Hole nodes increase, the model explains the effects of Black Hole attacks. However, the accuracy of the model decreases as the average node degree increases. Moreover, there is a discrepancy between the accuracy of predicting AODV and DSR Black Hole performance. The results suggest that there is a hidden behavioral difference in the route discovery process between the protocols or implementation of the Black Hole attack.

5.1.3 Analysis of Model Error

The significance of the modeling error over the entire experiment is examined to determine causality. The squared difference between the measured *Packet Loss Percentage* and the analytical model's prediction for AODV is shown in Figure 13. In this figure, the x-axis is the number of Black Holes, y-axis is the average node degree, and the z-axis is the squared difference between the experiment results and the analytical model.

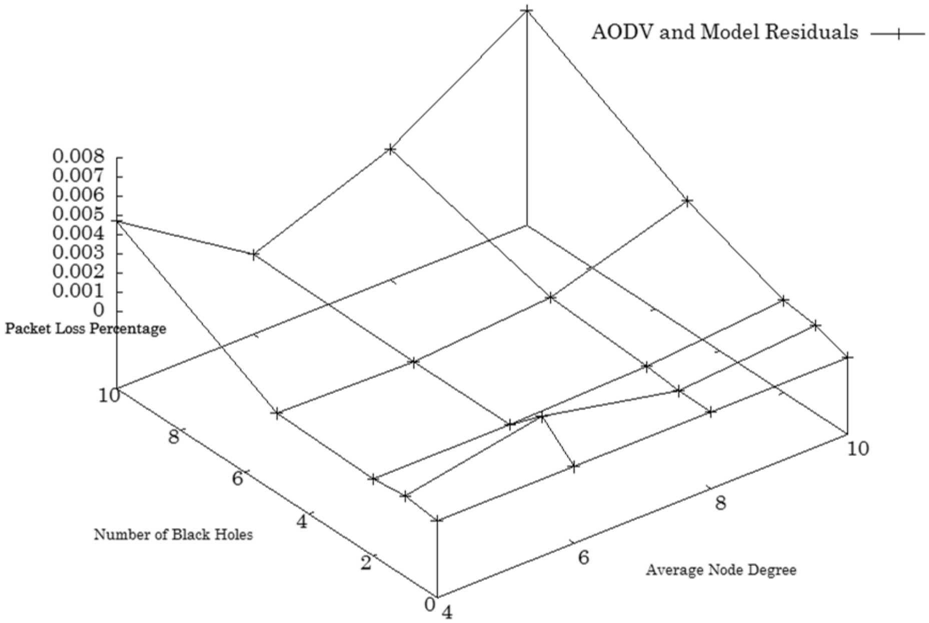

Figure 13: Residual Error of the Analytical Model and AODV

There are several observations to make about the surface of the error. With respect to the average node degree, error is minimized when the degree is 6. One explanation for the minimal error is because the number of nodes in the model is close to the number of nodes in the ad-hoc network. In this case, a 6-cube with 64 nodes is evaluated against the 40 node ad-hoc network. It is reasonable to believe this also causes the increase in error as the number of Black Holes increase. Recall that the analytical model uses random selection via hypergeometric distribution to determine the probability that at least one Black Hole node is in a favorable position to achieve an attack. Consider the case where the degree is 10 and the number of Black Holes is also 10 for a 40 node network. To achieve degree 10, the model assumes a 10-cube hypercube which has 1024 nodes. It is easy to realize that drawing 10 samples from a population of 1024 nodes has a vastly different density function than taking the same number of samples from a population of 40 nodes. This suggests that it is more important for the topology approximation to match the number of nodes than the average node degree.

Figure 14 shows the residual error between DSR experimental results and the analytical model. While the error is more significant between the model and the DSR Black Hole implementation, the error still decreases as the number of nodes in the model approaches the number of nodes in the experiment.

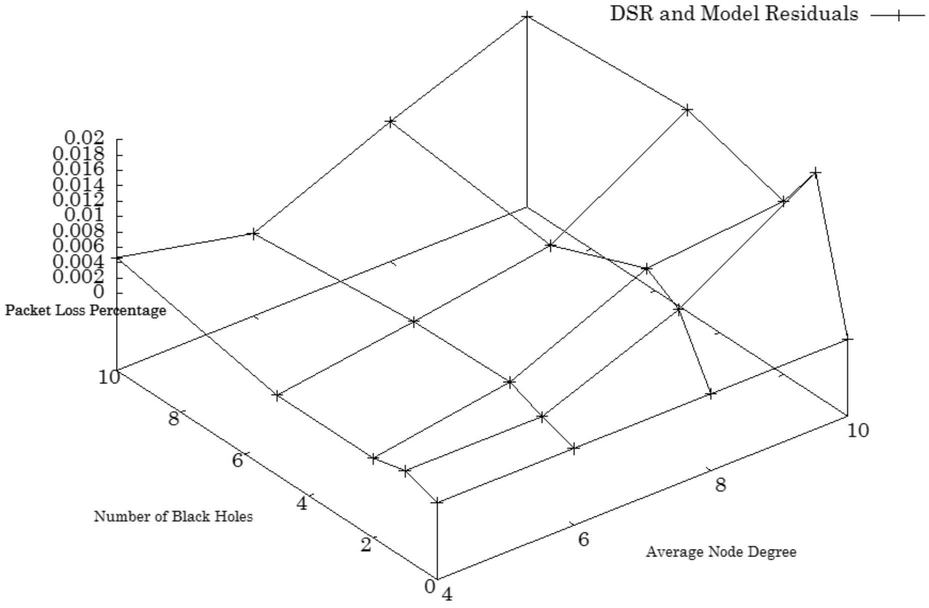

Figure 14: Residual Error of the Analytical Model and DSR

Two points of interest that deserve further explanation are the local anomalies in Figure 13 and Figure 14. For Figure 13, there is a local maximum where the number of Black Holes is 2 and the average node degree is 6. For Figure 14, there is a local minimum where the average degree is 10 and there are 2 Black Hole nodes. It is not clear if these points are due to Type-I error or hidden interactions not covered in the analytical model. Further experimentation is required to explain these anomalies.

5.2 Consideration of Number of Nodes as Alternative Network Parameter

The analysis of error in Section 5.1.3 suggests that it is more important to match the number of nodes than the node degree. In this section, rather than have the analytical model match the average node degree, all experimental data is compared against the analytical model results using a 5-cube hop-distance density function. The 5-cube provides the closest approximation to the actual number of nodes in the experiment. Figures 15 through 18 show the expected percentage of packet loss versus the experimental networks with average node degrees of 4, 6, 8, and 10 respectively.

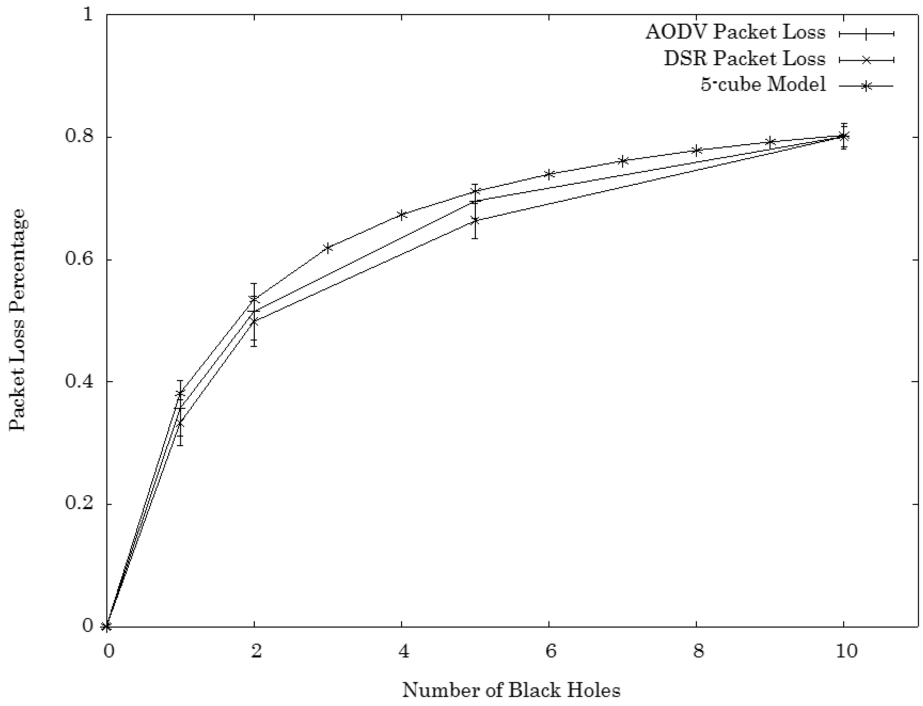

Figure 15: Packet Loss for 5-Cube model versus Ad-hoc Network with Average Node Degree 4

The results of this comparison are promising. The model's prediction falls within the 95% confidence interval for the majority of AODV samples. The exceptions are shown for the AODV *Packet Loss Percentage* for one Black Hole in Figure 16 and ten Black Holes in Figure 18. The first deviation between the model and the AODV Black Hole implementation can be explained by Type-I error due to sampling; however, the second one cannot. The significant deviation identifies the following possibilities: 1) there are interactions between Black Hole nodes that are not captured by the analytical model, 2) error increases as the average node degree deviates significantly from the degree of the analytical model, or 3) the border effects reduce the effectiveness of adding additional Black Holes.

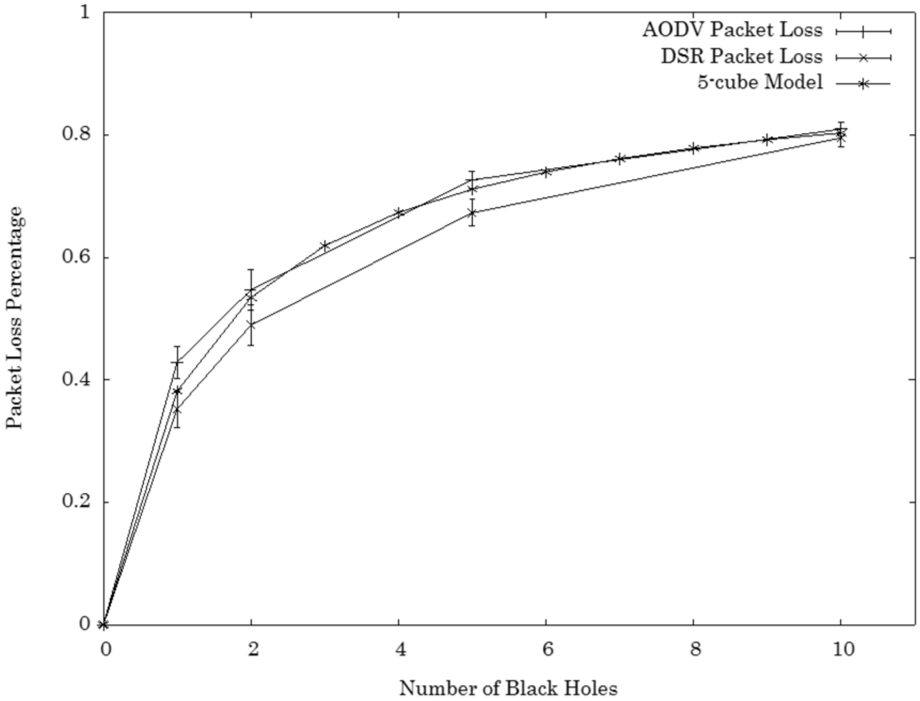

Figure 16: Packet Loss for 5-Cube model versus Ad-hoc Network with Average Node Degree 6

When observing the 5-cube model in comparison with the experimental results of the DSR Black Holes, the evidence that the analytical model predicts the effect is less compelling. While the 5-cube model follows the same order of growth as the simulation results, in the majority of cases the 5-cube significantly over-estimates the performance of DSR Black Holes. Moreover, the experimental results show that as the average node degree increases by decreasing the area, DSR Black Hole attack performance decreases. This may allude to the border effects discovered in [Bet02]. As the area decreases, the probability that an arbitrary node will encounter a border in the simulation increases. Since the hypercube model does not address border effects, it can be expected that an unbounded model will overestimate the performance of Black Hole attacks. What is not clear is why the border effect seems to affect DSR more than AODV.

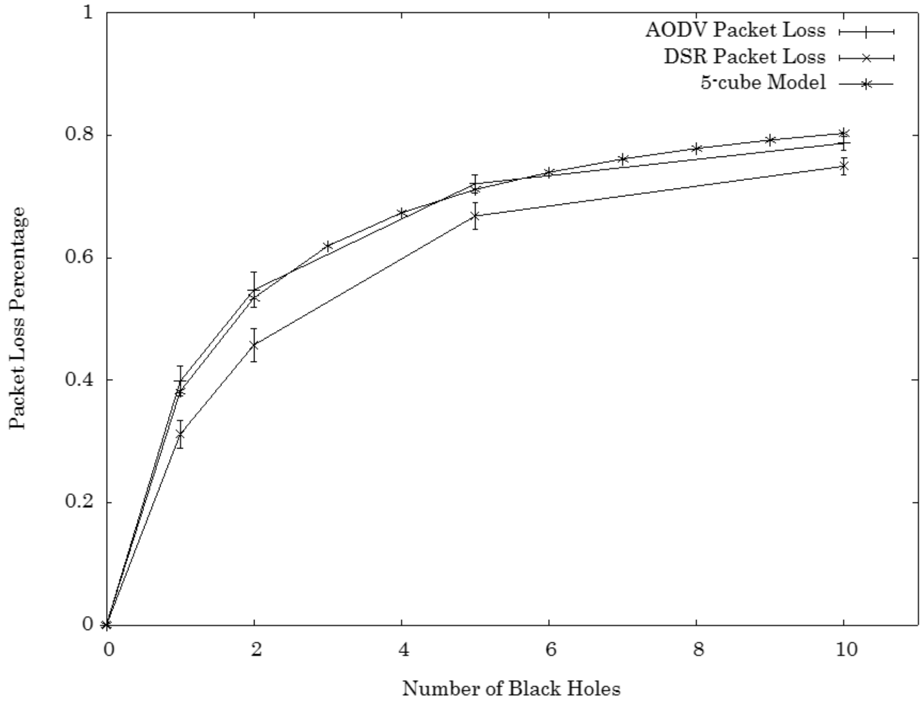

Figure 17: Packet Loss for 5-Cube model versus Ad-hoc Network with Average Degree 8

The main issue is that there is a significant difference in performance between the AODV and DSR Black Holes, making it difficult for an agnostic reactive protocol model to cover both protocols. This is surprising considering they utilize the same route discovery process, which includes the RREQ flooding and route selection criteria. Possible reasons for the difference include 1) there is an implementation difference in the NS-2 MANET protocol models, or 2) there is a difference between the implementations of the DSR and AODV Black Holes.

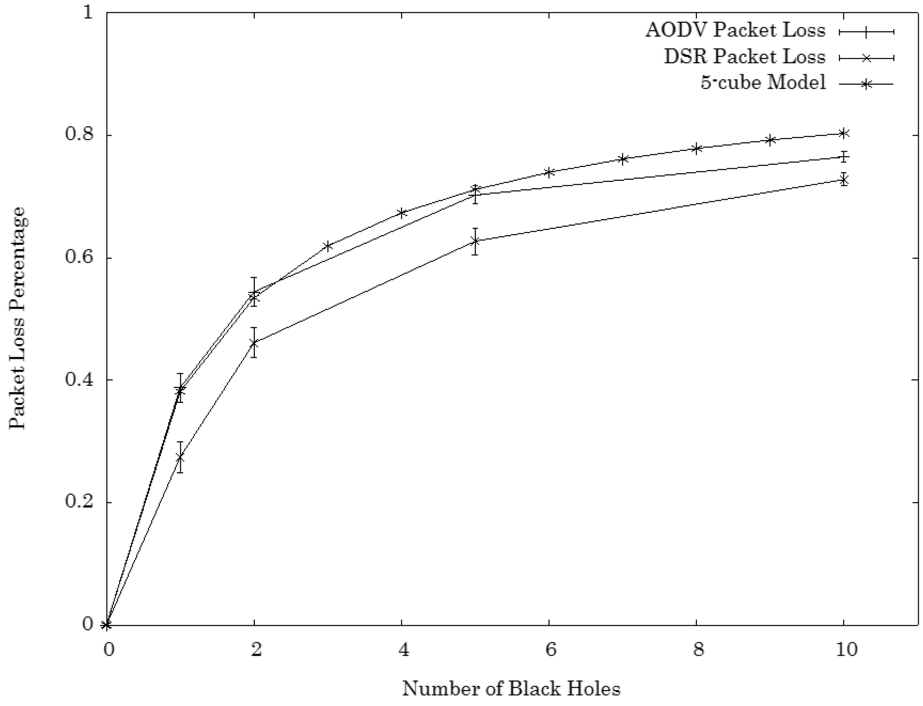

Figure 18: Packet Loss for 5-Cube model versus Ad-hoc Network with Average Node Degree 10

For completeness, the residuals of the experiment and a 5-cube are shown against the residuals experienced when the analytical model matched the average node degree of the experiment in Figures 19 and 20.

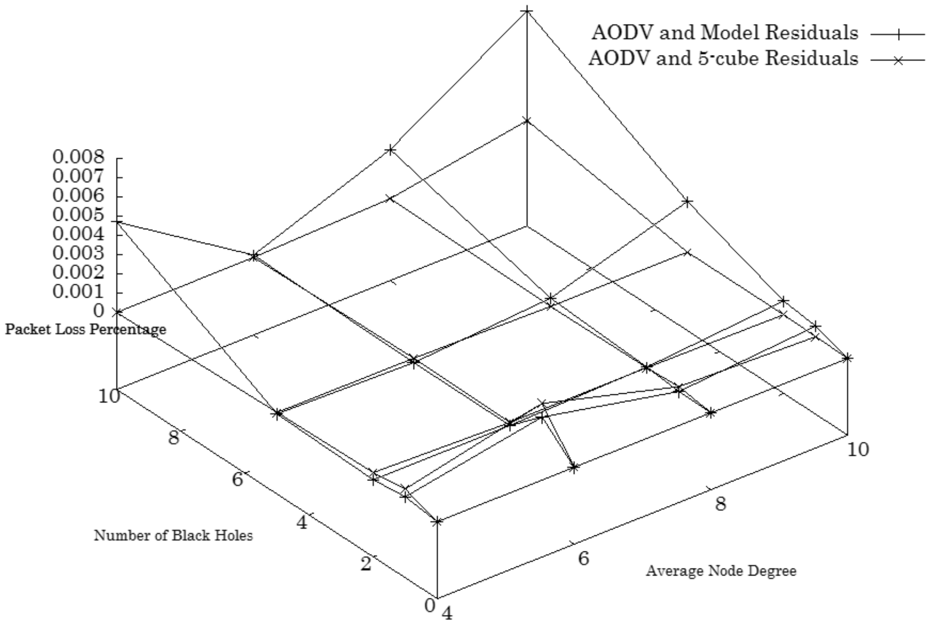

Figure 19: Residual Differential of 5-Cube Model for AODV

The figures provide evidence that using a hypercube topology to approximate the number of nodes in an ad-hoc network incurs less error than approximating the average node degree. The residuals against the 5-cube are generally less than the matching average node degree strategy. However, because the number of nodes is fixed to 40 for this experiment, a future experiment must be conducted to test this hypothesis against networks with different numbers of nodes to reach a valid conclusion on using this strategy.

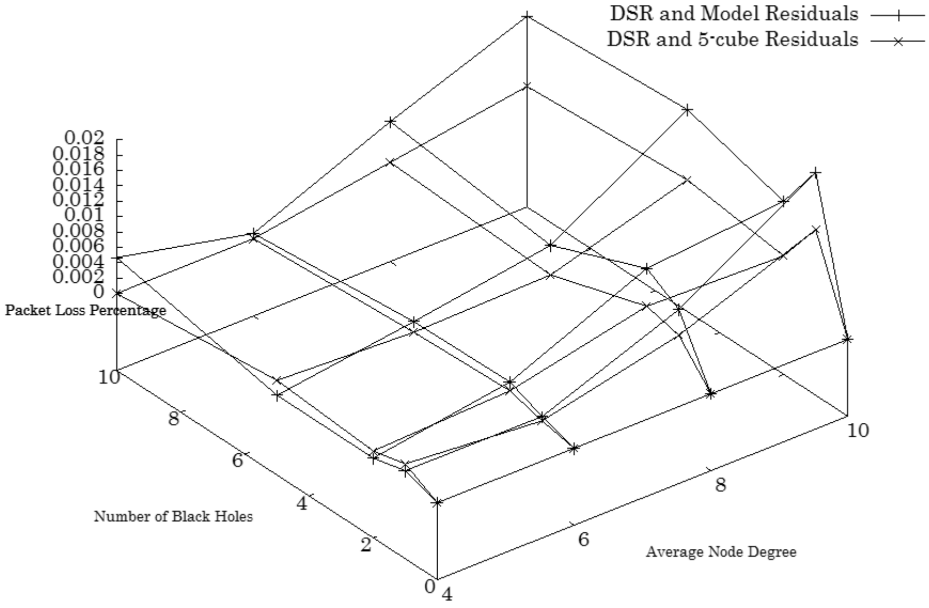

Figure 20: Residual Differential of 5-Cube Model for DSR

5.3 Summary of Findings

- The analytical model explains the main effects of Black Hole attacks on Reactive MANET protocols.
- The accuracy of the model is higher for AODV than DSR.
- The accuracy of the model improves as the number of nodes in the topology approximation approaches the actual number of nodes in the ad-hoc topology; suggesting that it is more important for the topology approximation to match the number of nodes than the degree.
- Inaccuracies of the analytical model may be explained by a mismatching of topology parameters between the hypercube approximation and the ad-hoc topology, border effects, hidden interactions between Black Hole nodes, and protocol or Black Hole implementation differences between DSR and AODV.

5.4 Conclusions on the Hypothesis

While the evidence in support of the hypothesis is not convincing, there is suggestive evidence that the analytical model predicts the performance loss of an ad-hoc network. Additional experimentation is required to isolate the causes of the observed prediction error and to enhance the analytical model accordingly.

VI. Conclusion

6.1 Summary of Work Performed

In this thesis the Black Hole attack is explored as an optimization problem with constraints, which includes the extent to which a Black Hole node can fabricate a lucrative route for a source node route discovery advertisement. Theorem 1 is developed for the shortest length falsified route. This theorem is used to derive Theorem 2, which is the predicate-logic that determines whether a Black Hole attack is successful or not.

While useful, the predicate requires *a-priori* knowledge about relative locations of the source, destination, and Black Hole nodes. To be able to evaluate ad-hoc topologies without knowing the relative distances for all of the nodes or the hop-distance density function of the topology, it was hypothesized that a simpler topology with similar network parameters could be substituted in place of the ad-hoc topology. Because of the symmetric qualities of the hypercube, the hop-distance density function is derived as a function of its degree. The probability density function for a hypercube is substituted for a target ad-hoc network with similar network parameters to enable the evaluation of Theorem 2. The application of the density function for hypercubes and Theorem 2 results in an analytical model that determines the probability an arbitrary route in a network is subject to Black Hole attack.

To evaluate the applicability of this analytical model, an experiment is conducted via simulation. The percentage of packet loss is measured for multiple ad-hoc network configurations including different MANET protocols, average node degree, and number of Black Hole nodes in the network. The results of the experiment show that the analytical model describes the probability of Black Hole attack; however, the model suffers from second-order interactions that are not considered in the model (e.g., protocol differences, interactions between Black Holes, etc.).

6.2 Accomplishments

There are several significant accomplishments of this thesis. First, two theorems are given to formalize limitations on Black Hole attacks for reactive MANET protocols that use hop-count to select routes. This work developed a predicate to explain the reason a Black Hole attack is successful or not for this class of network protocols. Second, simplifying network topologies via topology substitution is a completely new approach to solving network problems. Third, the hop-distance density function for hypercube topologies was developed using a recurrence relationship. Fourth, an alternative Black Hole analytical model to König's Black Hole model in Section 2.3.3.2 has been developed and tested under a variety of ad-hoc network configurations. This model has been shown to explain the general effect of Black Hole attacks and supports the proposed theorems for reactive MANET protocols in ad-hoc networks.

6.3 Recommendations for Future Work

While significant work has been accomplished for this thesis, it has also exposed areas ripe for additional exploration. This section provides direction for the near and far term plans within this thesis topic.

6.3.1 Near-term Plans

Work that should immediately follow this thesis includes 1) experiments to understand and characterize the model error, 2) determining which network parameters make the biggest impact in topology approximation, and 3) discovering the reason the AODV and DSR Black Hole performances are different.

6.3.2 Long-term Plans

Other work includes exploration of areas that were not covered by this thesis. First, the choice of using the hypercube interconnection network was purely from intuition. A useful experiment would be one that tests the hypothesis that this is the best topology for ad-hoc topology substitution instead of other interconnection networks (e.g., k-ary n-cubes, n-ary trees).

Second, while Section 3.2 explores the different constraints of Black Hole attacks, the analytical model only considers the limitations on falsification of coordination messages. One interesting and unexplored area is to model the effects of the self-imposed denial of service presented in Section 3.2.3. This model could determine the steady state number of routes that pass through a Black Hole.

Combining this model with the analytical model presented in this thesis will provide a more accurate prediction of effects.

Third, the thesis experiment tested the analytical model against a very simple network. Because the model does not consider the effects of congestion, route caching, flow routing, snooping, and mobility, they were omitted from the experiment. Moreover, hop-count is only considered in AODV if the sequence numbers match, so it would be beneficial to incorporate behaviors of sequence number guessing into an exclusive AODV version of the analytical model. Future work could focus on incorporating these elements into the model, or at least quantifying the accuracy of the existing model against networks with more complex functionality.

Fourth, there are some areas for improvement within the mathematics of the model with the goal of simplifying the calculation of expected network performance loss. For example, the recurrence relationship in the density function for the neighbor distance in a hypercube could be transformed into a closed-form differential equation using methods described in the Recurrences Chapter in [CLR04]. In addition, the analytical model produces a response that is logarithmic. It seems reasonable to expect that the effects of a Black Hole attack can be generalized using fitting methods as a logarithmic function.

Bibliography

[AHK04] I. Aad, J.-P. Hubaux, and E.W. Knightly. "Denial of service resilience in ad hoc networks." Proceedings of Mobicom. 2004. pp. 202-215.

[AHK08] I. Aad, J.-P. Hubaux, and E. W. Knightly. "Impact of Denial of Service Attacks on Ad Hoc Networks." IEEE/ACM Transactions on Networking, Vol 16, No 4, 2008: pp. 791-802.

[Bet02] C. Bettstetter."On the Minimum Node Degree and Connectivity of a Wireless Multihop Network." Proceedings of the 3rd AMC international symposium on Mobile ad hoc networking & computing. Lausanne, Switzerland: ACM, 2002. pp. 80-91.

[BeE03] C. Bettstetter, J. Eberspacher. "Hop Distances in Homogeneous Ad Hoc Networks." Vehicular Technology Conference. IEEE, 2003. pp. 2286-2290.

[BhS09] N. Bhalaji, and A. Shanmugam. "Association Between Nodes to Combat Blackhole Attack in DSR Based MANET." International Conference on Wireless and Optical Communications Networks. 2009. pp. 1-5.

[BJJ07] W. Bing, C. Jianmin, W. Jie, and M. Cardei. "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks." In Wireless Network Security, by Y. Xiao, X. Shen and D.-Z. Du, 103-136. New York, NY: Springer, 2007.

[CFG11] B. G. Constantine, G. Forget, R. Geib, and R. Schrage. Framework for TCP Throughput Testing. Internet Engineering Task Force Network Working Group, 2011. http://www.faqs.org/rfcs/rfc6349.html. Last accessed: Feb 7, 2012.

[ChP10] I. Chakeres, and C. Perkins. Dynamic MANET On-demand Routing version 21. Internet-Draft, Internet Engineering Task Force, 2010. http://tools.ietf.org/html/draft-ietf-manet-dymo-21. Last accessed: Feb, 7 2012.

[Cla88] D. Clark. "The design philosophy of the DARPA internet protocols." Symposium proceedings on Communications architectures and protocols. ACM, 1988. pp. 106-114.

[CLR04] T. Cormen, C. Leiserson, R. Rivest, and C. Stein. “Introduction to Algorithms” 5th Ed. Cambridge, Massachusetts: McGraw-Hill, 2004.

[CPZ09] J. Cai, , P. Yi, Y. Zhou, and N. Liu. "The Simulation and Comparison of Routing Attacks on DSR Protocol." International Conference on Wireless Communications, Networking and Mobile Computing. 2009. pp. 1-4.

[DhS08] A. Dhane, and S. Sharma. "Modeling and Analysis of Sequence Number Attack and its Detection in AODV." 16th IEEE International Conference on Networks. IEEE, 2008. pp. 1-6.

[DSE07] S. Dokurer, Y. M. Erten, and C. E. Acar. "Performance analysis of ad-hoc networks under black hole attacks." SoutheastCon. IEEE, 2007. 148-153.

[Fol11] Lt. Col. R. L. Folks. “Network Centric Operations in the Age of Cyberspace Operations.” Thesis, Carlisle Barracks: United States Army War College, 2011.

[FZJ09] Q. Feng, Z. Cai, J. Yang, and X. Hu. "A Performance Comparison of the Ad Hoc Network Protocols." Second International Workshop on Computer Science and Engineering. 2009. pp. 293-297.

[GAM07] E. Gerhards-Padilla, N. Aschenbruch, and P. Martini. "Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs." 32nd IEEE Conference on Local Computer Networks. 2007. pp. 1043-1049.

[GoY02] S. Gou, and O.W. Yang. "Performance of backup source routing in mobile ad hoc networks." Wireless Communications and Networking Conference, 2002. WCNC2002. 2002 IEEE. 2002. pp. 440-444.

[Hwa93] K. Hwang. "Advanced Computer Architecture: Parallelism, Scalability, Programmability." In 2.4 System Interconnect Architectures, 75-96. New York: McGraw-Hill, 1993.

[JHM07] D. Johnson, Y. Hu, and D. Maltz. The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks. IETF, 2007. http://www.ietf.org/rfc/rfc4728.txt. Last accessed: Feb 7, 2011

[JP 3-13] JP 3-13 Information Operations. Joint Publication, Defense Technical Information Center, 2006.

[KAD07] N. Kettaf, H. Abouaissa, T. Vu Duong, and P. Lorenz. Admission Control enabled On demand Routing (ACOR) version 3. Internet Standard Draft (Expired), Internet Engineering Task Force, 2007. http://tools.ietf.org/html/draft-kettaf-manet-acor-03. Last accessed: Feb 7, 2011.

[KGA06] S. Khurana, N. Gumpta, and N. Aneja. "Reliable Ad-hoc On-demand Distance Vector Routing Protocol." Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. International Conference on. 2006. pp. 98.

[KHK09] A. König, M. Hollick, T. Krop, and R. Steinmetz. "GeoSec: quarantine zones for mobile ad hoc networks." Security and Communications Networks. Wiley InterScience, 2009. pp. 271-288.

[KiL07] D. Kiwior, and L. Lam. "Routing Protocol Performance Over Intermittent Links." MITRE, 2007. http://www.mitre.org/work/tech_papers/tech_papers_07/07_0778/07_0778.pdf. Last accessed: Feb 7, 2012.

[KSS09] A. König, D. Seither, R. Steinmetz, and M. Hollick. "An Analytical Model of Routing, Misbehavior, and Countermeasures in Mobile Ad Hoc Networks." Global Telecommunications Conference. IEEE, 2009. pp. 1-6.

[Lun00] J. Lundberg. "Routing Security in Ad Hoc Networks." Seminar on Network Security. 2000. pp. 1-12.

[MiA03] S. J. Milton, and J. C. Arnold. "Introduction to Probability and Statistics: Principles and Applications for Engineering and the Computing Sciences." New York: McGraw-Hill, 2003.

[Net11] The Network Simulator. September 13, 2011. http://www.isi.edu/nsnam/ns/. Last accessed September 13, 2011.

[OYM02] R. Onishi, S. Yamaguchi, H. Morino, H. Aida, and T. Saito. "The Multi-agent System for Dynamic Network Routing." Proceedings on the 5th International Symposium on Autonomous Decentralized Systems. 2002. pp. 375-382.

[PBD03] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing RFC-3561. IETF, 2003. http://www.ietf.org/rfc/rfc3561.txt. Last accessed Feb 7, 2012.

[PSA09] A. Prathapani, L. Santhanam, and P. Agrawal. "Intelligent Honeypot Agent for Blackhole Attack Detection in Wireless Mesh Networks." 6th International Conference on Mobile Adhoc and Sensor Systems. 2009. pp. 753-758.

[Ric00] Rice Monarch Project. Implementation of DSR. April 25, 2000. http://www.monarch.cs.rice.edu/dsr-impl.html. Last accessed Sep 13, 2011.

[SaS88] Y. Saad, and M. H. Schultz. "Topological Properties of Hypercubes." IEEE Transactions on Computers, 1988: pp. 867-872.

[Son09] A. Song. picoNet. July 17, 2009. http://sourceforge.net/projects/piconet/ (accessed September 13, 2011).

[Ste94] W. Stevens. "TCP/IP Illustrated Volume 1." In The Protocols, by W. Stevens, 297-306. Addison-Wesley, 1994.

[TAC09] M. Tiwari, K.V. Arya, R. Choudhari, and K. S. Choudhary. "Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information." Fourth International Conference on Computer Sciences and Convergence Information Technology. 2009. pp. 824-828.

[YaM03] P. Yau, and C. Mitchell. "Security Vulnerabilities in Ad Hoc Networks." Proceedings of the 7th International Symposium on Communication Theory and Applications. Ambleside, UK, 2003. pp. 99-104.

[ZPY10] S. Zhan, Y. Peng, Y. Yang, and J. Li. "An Open Architecture for the Routing Protocols Design in Ad Hoc Networks." IEEE International Conference on Computer Science and Information Technology. 2010. pp. 18-22.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMBNo. 074-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to an penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)* 22-03-2012	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From – To)* June 2008 – March 2012

TITLE AND SUBTITLE A BLACK HOLE ATTACK MODEL FOR REACTIVE AD-HOC PROTOCOLS	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Mr. Badenhop, Christopher W.	**5d. PROJECT NUMBER** 12G289
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/ENY) 2950 Hobson Way, Building 640 WPAFB OH 45433-8865	**8. PERFORMING ORGANIZATION REPORT NUMBER** AFIT/GCO/ENG/12-01
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Air Force Research Laboratory (AFRL/RYWC) BLD 620 2241 Avionics Circle WPAFB, OH 45433 937-528-8140 Juan.carbonell@wpafb.af.mil POC: Juan Carbonell, Branch Chief	**10. SPONSOR/MONITOR'S ACRONYM(S)** **AFRL/RYWC (AFMC)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES
This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT

Net-Centric Warfare places the network in the center of all operations, making it a critical resource to attack and defend during wartime. This thesis examines one particular network attack, the Black Hole attack, to determine if an analytical model can be used to predict the impact of this attack on ad-hoc networks. An analytical Black Hole attack model is developed for reactive ad-hoc network protocols DSR and AODV. To simplify topology analysis, a hypercube topology is used to approximate ad-hoc topologies that have the same average node degree. An experiment is conducted to compare the predicted results of the analytical model against simulated Black Hole attacks on a variety of ad-hoc networks. The results show that the model describes the general order of growth in Black Hole attacks as a function of the number of Black Holes in a given network. The model accuracy maximizes when both the hypercube approximation matches the average degree and number of nodes of the ad-hoc topology. For this case, the model falls within the 95% confidence intervals of the estimated network performance loss for 17 out of 20 measured scenarios for AODV and 7 out of 20 for DSR.

15. SUBJECT TERMS
Network availability, Black Hole attack, hop-distance density function, ad-hoc networks

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Barry Mullins, ADVISOR
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(Include area code)*
U	U	U	UU	113	785-3636 x7979 (barry.mullins@afit.edu)